GIBSON DUNN

Challenges in Compliance and Corporate Governance

January 29, 2019

Panelists:

F. Joseph Warin
M. Kendall Day
Sacha Harber-Kelly
Stuart F. Delery
Adam M. Smith
Lori Zyskowski

MCLE Certificate Information

MCLE Certificate Information

- Most participants should anticipate receiving their certificate of attendance in four weeks following the webcast.
- Virginia Bar Association members should anticipate receiving their certificate of attendance in six weeks following the webcast.
- All questions regarding MCLE Information should be directed to Jeanine McKeown (National Training Administrator) at 213-229-7140 or jmckeown@gibsondunn.com.

Presentation Overview

1	2	3	4	5
2018 in Brief: What You Should Know	U.S. Agencies Update: Personnel, Priorities, Penalties	Global Enforcement and Regulatory Developments	Focus on Gatekeepers	Building & Overseeing Effective Compliance

GIBSON DUNN

2018 in Brief

Enforcement: What's Changed and What Hasn't

- In the first two years of the Trump Administration, regulatory agencies have devoted resources and attention to many of the same priorities as in previous years.
  - **Cybersecurity** and **data privacy** continue to be areas of focus for corporations and enforcement authorities alike in the wake of numerous announcements in 2018 of large-scale private and public sector data breaches.
- The increasing attention by foreign regulators to potential cross-border misconduct has meant that companies must continue working to manage expectations both at home and abroad.
- Enforcement levels saw a slight decrease this year overall, although closer examination indicates a more nuanced picture:
  - Criminal enforcement remains robust.
  - Decline in civil enforcement, *e.g.*, with respect to False Claims Act and environmental matters.

Continuing Cross-Border Cooperation

- U.S. enforcers continue to voice strong support for international cooperation and coordinated, global resolutions, and 2018 witnessed significant international cooperation efforts.
  - U.S. authorities jointly investigated and negotiated corporate resolutions with new and longstanding partners alike, achieving global resolutions in anti-corruption, antitrust, anti-money laundering, and other matters.
- In May, the U.S. Department of Justice ("DOJ") announced a new (anti)-"Piling On" policy to encourage effective and fair cooperation among U.S. authorities at federal, state, and local levels, as well as with foreign counterparts.
- Corporations continue to face significant challenges in navigating parallel investigations and enforcement by international regulators, particularly with respect to issues of privilege, data privacy, and cooperation with law enforcement.
  - For example, recent blocking statutes in certain countries such as China have complicated considerations regarding cooperation with U.S. government investigations.

"[T]ransnational corruption and manipulation of our markets will be met with a global and coordinated law enforcement response."

– John P. Cronan, Principal Deputy Assistant Attorney General, June 4, 2018

Shifting Transnational Alliances

- This year has seen changes in alliances as a result of, among other political changes, the UK's move toward Brexit and President Trump's promotion of his "America First" foreign policy.

- Notable developments include:
  - DOJ announced its "China Initiative" on November 1. The initiative prioritizes countering economic espionage by Chinese companies and nationals.
  - The Brexit deal proposed by UK Prime Minister Theresa May could affect the UK's trade deal with the United States.
  - The Trump Administration made an historic foray into negotiations with North Korea, with a second summit planned for February 2019.
  - Countries have come together to counter U.S. sanctions, including efforts by China, the EU, and Russia to sidestep U.S. sanctions on Iran.

Role of State Enforcers

- State enforcement authorities were active in 2018, utilizing a broad complement of tools.
- State enforcers showcased their intent to play a continuing role alongside—and, sometimes, in lieu of—federal enforcement.
  - –New York's Department of Financial Services ("DFS") remains a major player.
  - –Regulators from a wide range of states have taken action, particularly with respect to data privacy and security.
- California, Illinois, Massachusetts, and New York are filling gaps created by decreased federal government enforcement.

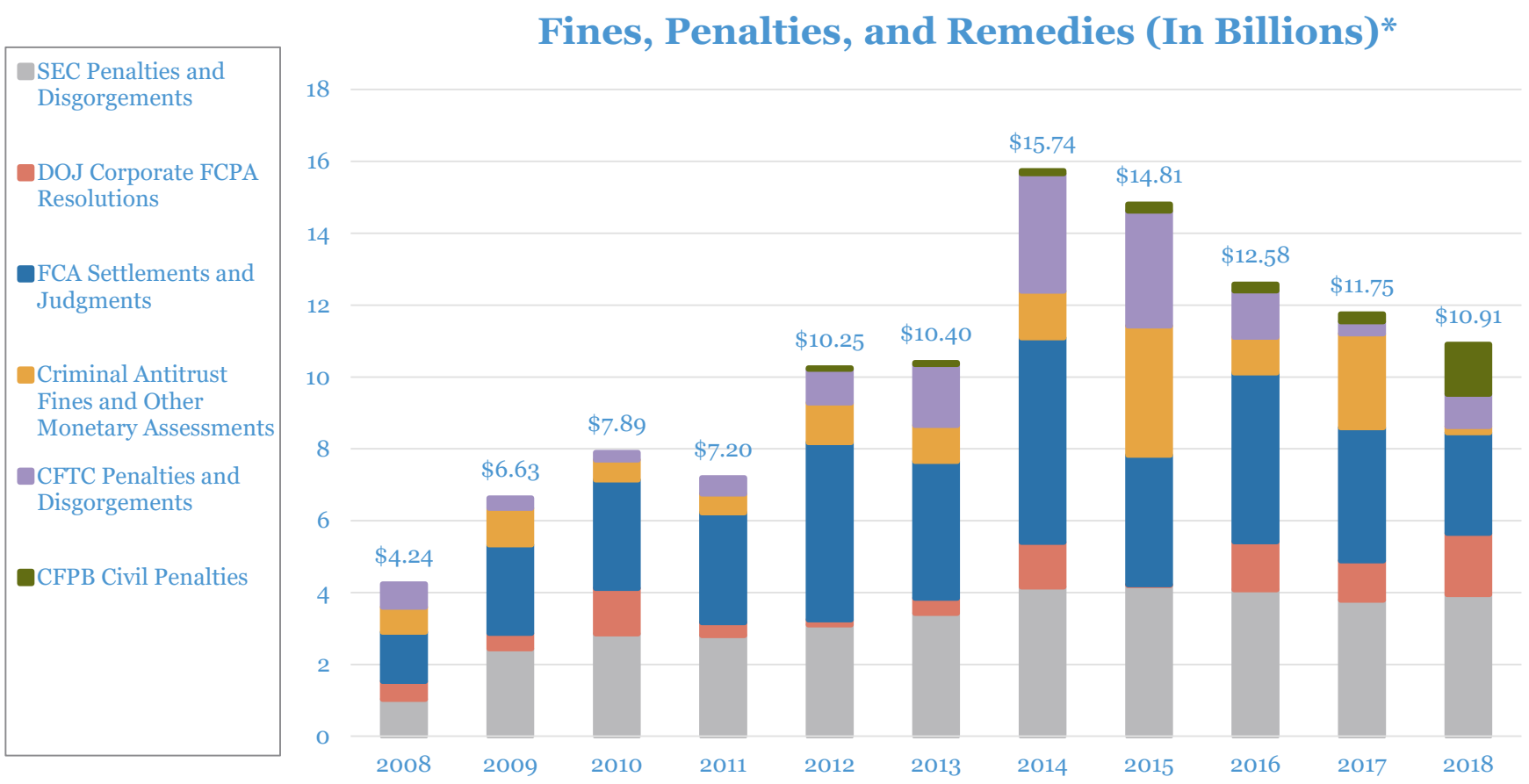
"In an era of weakened federal government oversight, strong state regulation is essential in order to safeguard our markets, ensure strong consumer protections and hold regulated entities accountable for their actions. New York will continue to lead in supporting a robust state financial services regulatory regime."

– Maria T. Vullo, New York DFS Superintendent, June 27, 2018

GIBSON DUNN

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

U.S. Fines Decrease



GIBSON DUNN

* GDC Internal Aggregations. CFPB Civil Penalties does not include CFPB recoveries and restitutions. CFPB recoveries and restitutions were included in prior iterations of this graphic. All figures are tracked by fiscal year except for DOJ Corporate FCPA resolutions, which are tracked by calendar year.

Top 2018 Fines and Penalties

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

Amount	Industry/Company	Area
$4.9B	Financial services institution	FIRREA
$2.09B	Financial services institution	FIRREA
$2B	Financial services institution	FIRREA
$1.3B	Financial services institution	Sanctions (DOJ, Federal Reserve, OFAC, NY DA, NY DFS)
$860M	Financial services institution	Antitrust, FCPA (DOJ, SEC, and local authorities)
$853M	South American oil and gas company	FCPA (DOJ, SEC, and local authorities*)
$765M	Financial services institution	FIRREA
$625M	U.S. pharmaceutical distribution company	False Claims Act
$280M	U.S. subsidiary of an Asian electronics manufacturer	FCPA (DOJ and SEC)
$270M	U.S. independent physician association	False Claims Act
$260M	U.S. hospital chain	False Claims Act
$149.5M	Global professional services company	False Claims Act
$90M	Financial services institution	Antitrust

* U.S. resolution credits non-punitive payments to local authorities for social responsibility programs pursuant to an agreement that does not include any findings of liability under local law.

Details on DOJ Enforcement in 2018

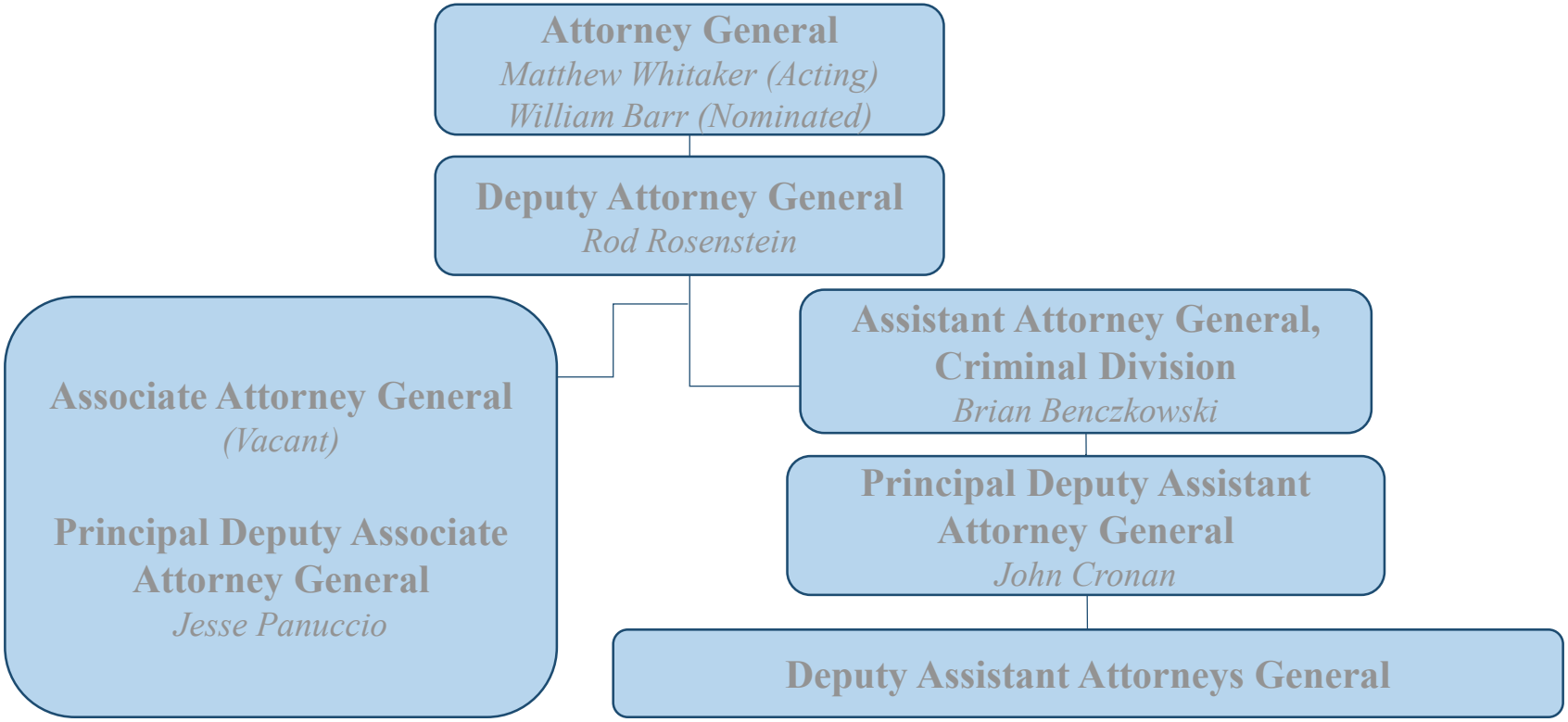
Key 2018 Enforcement

- Attorney General Jeff Sessions resigned in November.
- DOJ announced a number of significant policy changes relevant to corporate enforcement actions, including:
  - Potential expansion of the Foreign Corrupt Practices Act ("FCPA") Corporate Enforcement Policy to other areas of law;
  - Policy against "piling on" to encourage coordinated multi-agency resolutions;
  - Comprehensive revision to and update of U.S. Attorneys' Manual, now known as the "Justice Manual";
  - Changes to DOJ's policy regarding the selection of corporate monitors; and
  - Revisions to the individual accountability policies for corporate wrongdoing announced in the 2015 "Yates Memo."
- DOJ continues to coordinate closely with other federal, state, and international agencies to investigate and resolve transnational matters.

Details on DOJ Enforcement in 2018

Changes in Top Leadership

- Although DOJ has made considerable progress in filling in its leadership this year, several high-profile vacancies remain, including for Associate Attorney General (no nominee) and Assistant Attorney General for the Tax Division (no nominee).



Details on DOJ Enforcement in 2018

DOJ's New Anti-Piling On Policy

- In May, DOJ announced a new policy regarding the coordination of corporate resolution penalties to "discourage disproportionate enforcement of laws by multiple authorities."
- This new policy has been added to the Justice Manual and encourages DOJ to "consider the totality of fines, penalties, and/or forfeiture imposed by" other enforcement agencies to reach a fair and reasonable result. It specifically encourages DOJ attorneys to "coordinate with . . . other federal, state, local, and foreign enforcement authorities seeking to resolve a case with a company for the same misconduct."
- The policy does not bind other agencies.

"'Piling on' can deprive a company of the benefits of certainty and finality ordinarily available through a full and final settlement. We need to consider the impact on innocent employees, customers, and investors who seek to resolve problems and move on. We need to think about whether devoting resources to additional enforcement against an old scheme is more valuable than fighting a new one."

– Rod J. Rosenstein,
Deputy Attorney General,
May 9, 2018

Details on DOJ Enforcement in 2018

Revisions to DOJ's Corporate Monitor Selection Policy

- In a memorandum issued in October, Assistant Attorney General Brian Benczkowski articulated a modified approach to corporate monitorships.
- The Benczkowski Memo also put in place a more robust process for selecting independent compliance monitors to protect the integrity and transparency of the process.
- Benczkowski announced that the Criminal Division was discontinuing its use of a single compliance counsel, a position created in 2015.

Key Principles of New DOJ Monitor Guidance

- Corporate monitorships should not be punitive, but rather oriented toward ensuring compliance with a resolution and preventing future misconduct;
- The decision whether to impose a monitor should be based on the nature of the misconduct and its pervasiveness throughout the organization;
- Prosecutors should hesitate to impose a monitor based on an inadequate compliance environment that no longer exists, or a prior leadership team; and
- Prosecutors should consider financial costs and other burdens to the organization associated with retaining and maintaining a corporate monitor.

Details on DOJ Enforcement in 2018

Revisions to Individual Accountability Policy

- In November, DOJ announced a series of significant modifications to its policy regarding individual accountability in corporate enforcement actions (as set forth in the Yates Memo); these changes have been incorporated into the revised Justice Manual.
- Features of the new guidance include:
  - –Lowering the threshold for maximum cooperation credit from disclosing all involved individuals to only substantially involved individuals;
  - –Granting civil litigators greater discretion to determine an appropriate amount of cooperation credit; and
  - –Allowing civil attorneys to consider a defendant's ability to pay in deciding whether to pursue a civil judgment.
- The revised guidance reflects concerns about the investigative burden imposed on defendants by the prior, more open-ended requirements.
- DOJ has not yet clarified the interplay between this new policy and the FCPA Corporate Enforcement Policy.

"'When the government alleges violations that involved activities throughout the company over a long period of time, it is not practical to require the company to identify every employee who played any role in the conduct . . . Our policies need to work in the real world of limited investigative resources."

– Rod J. Rosenstein,
Deputy Attorney General,
Nov. 29, 2018

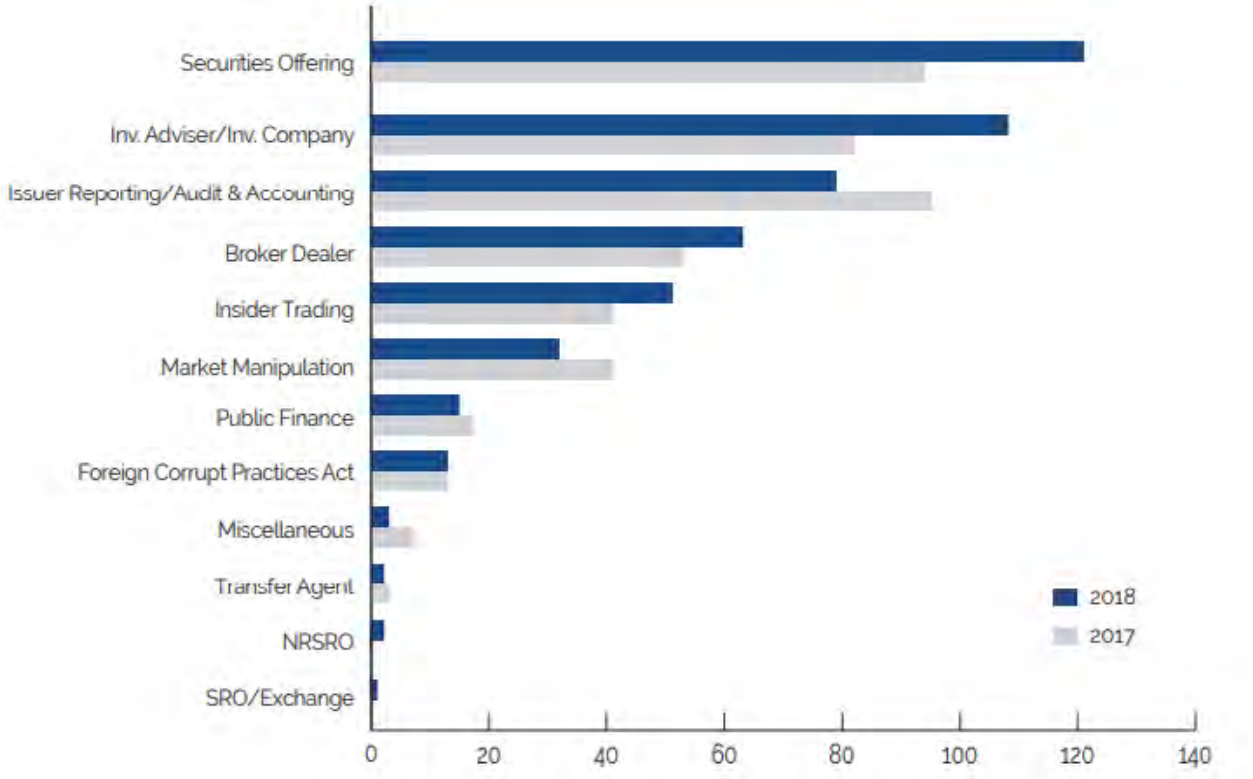
Details on SEC Enforcement in 2018

Review of Key Focus Areas for SEC Enforcement

- The Division of Enforcement's 2018 Annual Report reflects on the U.S. Securities and Exchange Commission's ("SEC") efforts with respect to five key focus areas:

1. Protecting the Main Street investor;
2. Pursuing individual accountability;
3. Keeping pace with technological change;
4. Imposing sanctions that most effectively further enforcement goals; and
5. Constantly assessing its allocation of resources.

Types of Cases (SEC Standalone Actions)



SEC Division of Enforcement 2018 Annual Report

Details on SEC Enforcement in 2018

Key 2018 Developments

- In February, the SEC issued an interpretive release updating its 2011 guidance to public companies regarding the disclosure of cybersecurity risks and incidents. The release:
  - –Confirmed that materiality analysis should be understood similarly to other contexts;
  - –Stated that public companies must disclose the board risk oversight role (including regarding cybersecurity) in proxy statements; and
  - –Emphasized vigilance in protecting material non-public information regarding cyber issues.
- In a May speech, Commissioner Peirce discussed the SEC's shift away from a "broken windows" enforcement model towards a sharper focus on high-priority cases.
- In September, Chairman Clayton affirmed the SEC's position that Staff statements are nonbinding and create no enforceable legal rights or obligations.
- In November, the SEC announced its first enforcement action against a digital token trading platform on the basis that it was operating as an unregistered national securities exchange.

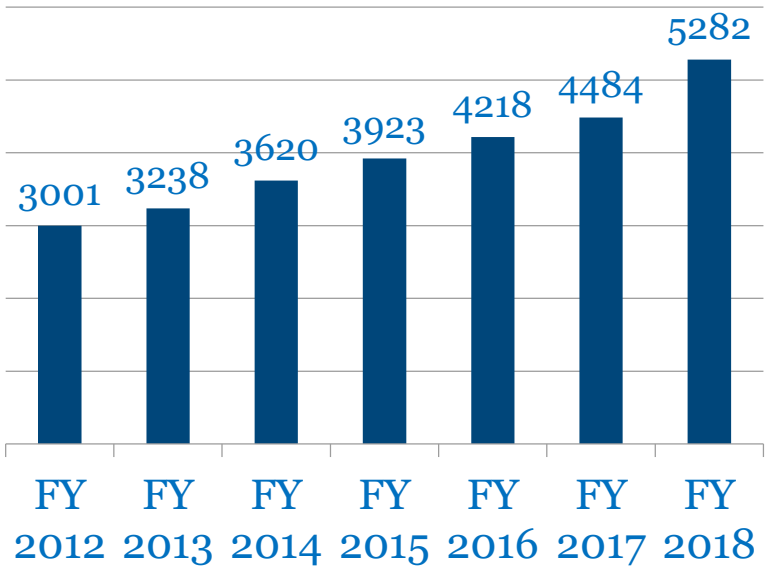
"Today, the SEC, no longer measuring its success by tallying up enforcement statistics, is making a more concerted effort to bring only meaningful enforcement actions. . . . Our goal is not to investigate for the sake of investigating, but to protect the capital markets by focusing our efforts on the enforcement actions with the biggest impact."

– Hester M. Peirce,
SEC Commissioner,
May 11, 2018

Details on SEC Enforcement in 2018

Whistleblower Update

- In FY 2018, the SEC received a record-shattering 5,282 tips, a 17.8% increase from FY 2017.
  - –Consistent with previous years, the most common complaint categories were:
    - Offering fraud (20%);
    - Corporate disclosures and financials (19%); and
    - Manipulation (12%).
  - –In addition to U.S.-based tips, the SEC received tips from individuals in 72 different countries in FY 2018.
- The SEC reported that it paid approximately $168 million to 13 individuals in FY 2018, including the three largest awards in the program's history. Since the program's inception, the SEC has issued more than $362 million in awards.
- In June, the SEC proposed a substantial set of amendments to its whistleblower program; these amendments remain under consideration.

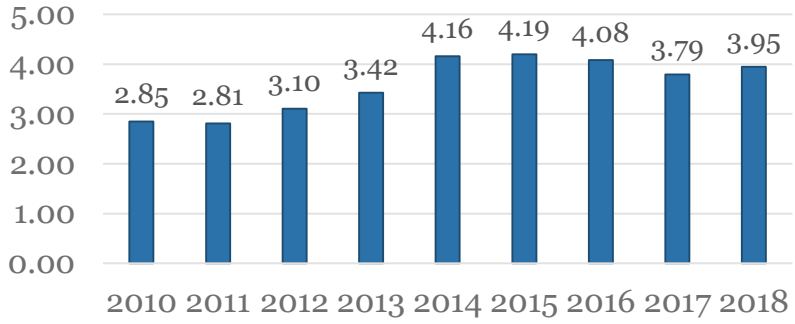


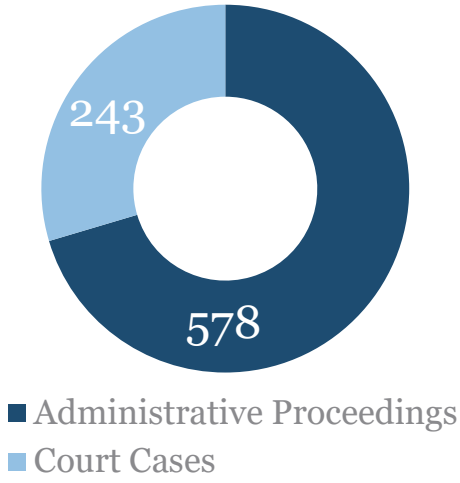
Details on SEC Enforcement in 2018

Key 2018 Cases

- In *Somers v. Digital Realty Trust*, the Supreme Court held 9-0 that the Dodd-Frank anti-retaliation provision applies only to whistleblowers who report their concerns to the SEC, not to those who only file internal reports.
- In *Lucia v. SEC*, the Supreme Court held in a 7-2 decision that the SEC's administrative law judges ("ALJ") are "officers of the United States," and thereby subject to the Appointments Clause of the Constitution.
  - As a result, the SEC agreed to rehear more than 128 cases previously litigated before ALJs found to have been improperly appointed; the full Commission reaffirmed the ALJ appointments in compliance with the ruling.
- In December, the Supreme Court heard oral argument in *Lorenzo v. SEC*, a case on appeal from the D.C. Circuit regarding the scope of scheme liability under Rule 10b-5.
  - The petitioner claims that he cannot be found liable under a theory of "scheme" liability for distributing a misstatement of which he was not the "maker" under the *Janus* standard.

SEC Penalties and Disgorgements (in billions)

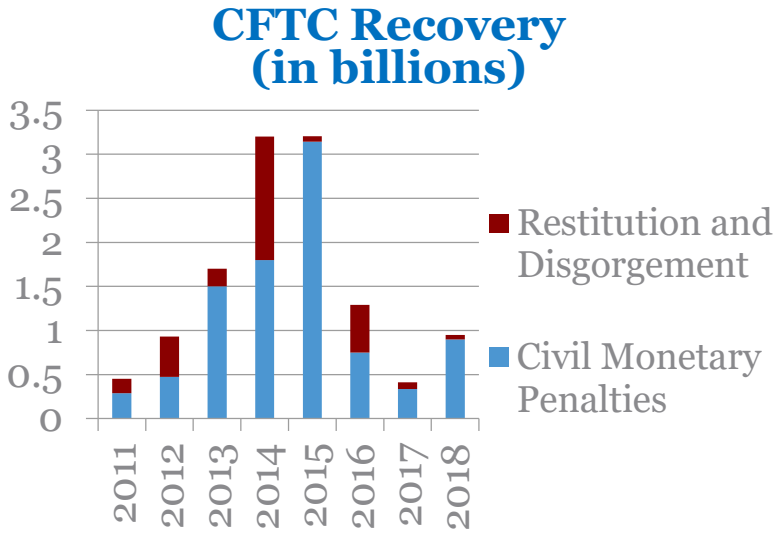




Details on CFTC Enforcement in 2018

Key Statistics and Trends

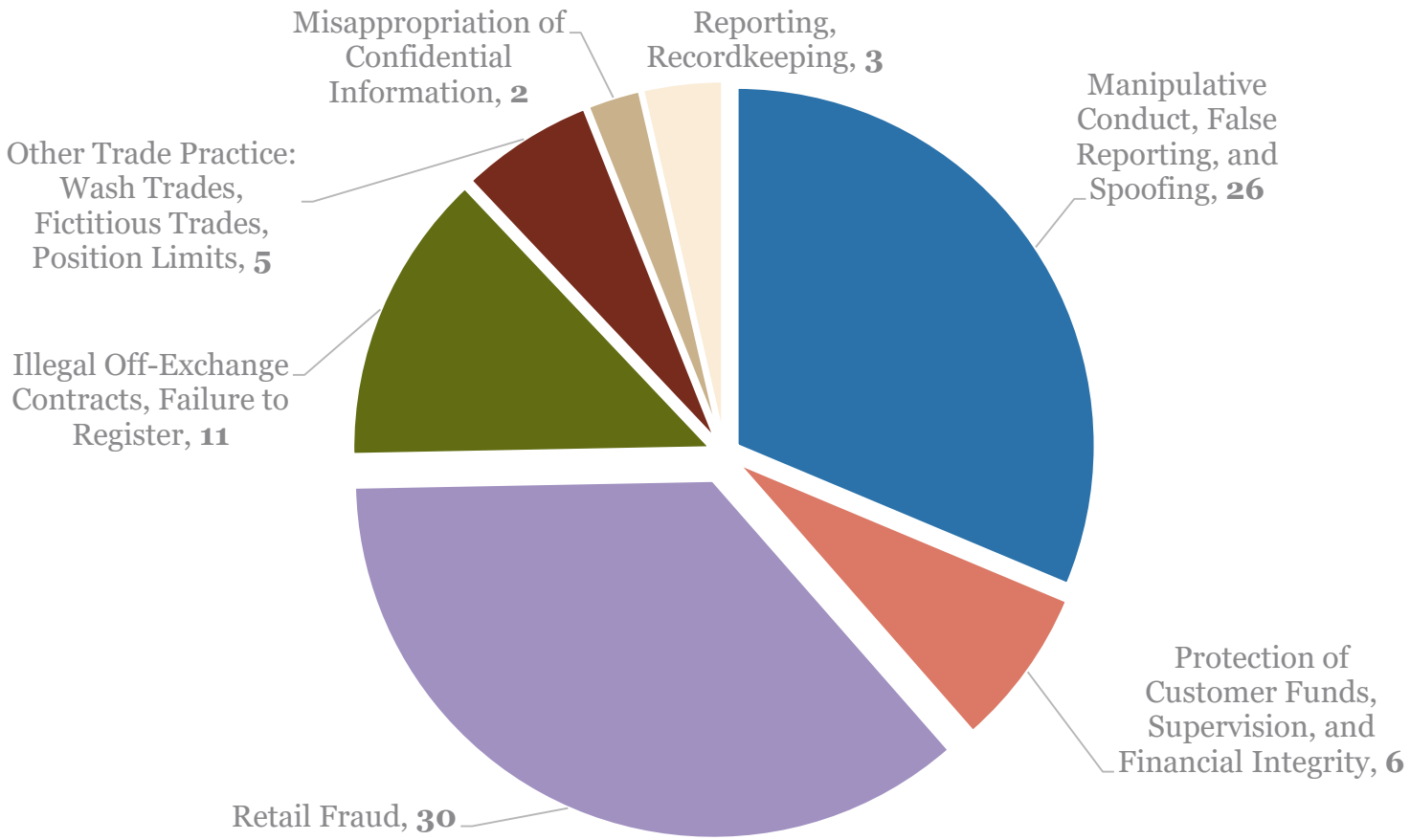
- In 2018, the Commodity Futures Trading Commission ("CFTC"):
  - Brought 83 enforcement-related actions, a substantial increase from 49 enforcement actions filed in 2017;
  - Imposed monetary judgments of $10 million or more in ten cases, more than in any other year; and
  - Aggressively pursued wrongdoing involving trading misconduct, such as manipulation, spoofing, and wash trading.



- To advance its priorities, the CFTC created specialized task forces in four substantive areas: Spoofing and Manipulative Trading; Virtual Currency; Insider Trading and Protection of Confidential Information; and Bank Secrecy Act ("BSA").
- The CFTC Division of Enforcement's 2017 cooperation advisories manifested in some reduced penalties in 2018. In several spoofing enforcement actions, the CFTC specifically noted that the companies received credit for substantial cooperation and self-reporting.

Details on CFTC Enforcement in 2018

2018 Enforcement Actions by Category



https://www.cftc.gov/sites/default/files/2018-11/ENFAnnualReport111418_0.pdf

FinCEN Update

- The Financial Crimes Enforcement Network ("FinCEN") had another active year:
  - –FinCEN issued a finding and notice of proposed rulemaking under Section 311 of the USA PATRIOT Act to declare a Latvian Bank, ABLV Bank, an institution of primary money laundering concern. ABLV subsequently liquidated itself.
  - –FinCEN assessed a $185,000,000 penalty against U.S. Bank for AML failures.
  - –The "Customer Due Diligence" rule became effective in May.
  - –FinCEN expanded the coverage of Geographic Targeting Orders ("GTO") from 6 cities to 12: Boston; Chicago; Dallas-Fort Worth; Honolulu; Las Vegas; Los Angeles; Miami; New York City; San Antonio; San Diego; San Francisco; and Seattle. The threshold is also now set at $300,000 for all cities and covers purchases made using virtual currencies.
  - –FinCEN continues to play an important role in interagency law enforcement efforts:
    - Nearly 500 federal, state, and local agencies have access to FinCEN's database of BSA records.
    - FinCEN receives more than 1,500 Suspicious Activity Reports ("SAR") related to virtual currency transactions each month.
    - FinCEN receives nearly 1,900 SARs related to terrorist financing each year.

PCAOB Update

- 2018 brought a notable decrease in settled PCAOB enforcement orders, from more than 50 in 2017 to 20 in 2018, potentially linked to personnel turnover.
- There was significant turnover of senior divisional and office leadership in 2018—including the General Counsel, the Director of Enforcement and Investigations, and the Director or Registration and Inspections—creating uncertainty about the status of initiatives and future divisional efforts.

> *"We're also considering difficult questions surrounding our approach to defining and presenting inspection findings, as well as the content and geography of matters presented in our inspection reports."*
>
> - William D. Duhnke, PCAOB Chairman, May 17, 2018

- In November, PCAOB approved a five-year strategic plan, which is part of a larger effort by the new PCAOB board members to rethink PCAOB processes and initiatives. The greatest focus is on increasing the speed and relevance of inspection reports.
- PCAOB spent significant time in 2018 assessing how Critical Audit Matters ("CAMs") should be identified and disclosed, as 2019 will be the first year that CAMs will be disclosed by auditors of the largest companies.

GIBSON DUNN

Global Enforcement and Regulatory Developments

Global Enforcement and Regulatory Developments

- Sanctions
- Data Privacy and Security
- BSA/AML
- Governance
- White Collar and Securities Fraud
- Antitrust
- False Claims Act
- Environmental
- Criminal Tax and Cross-Border Concerns

Sanctions
U.S. Update

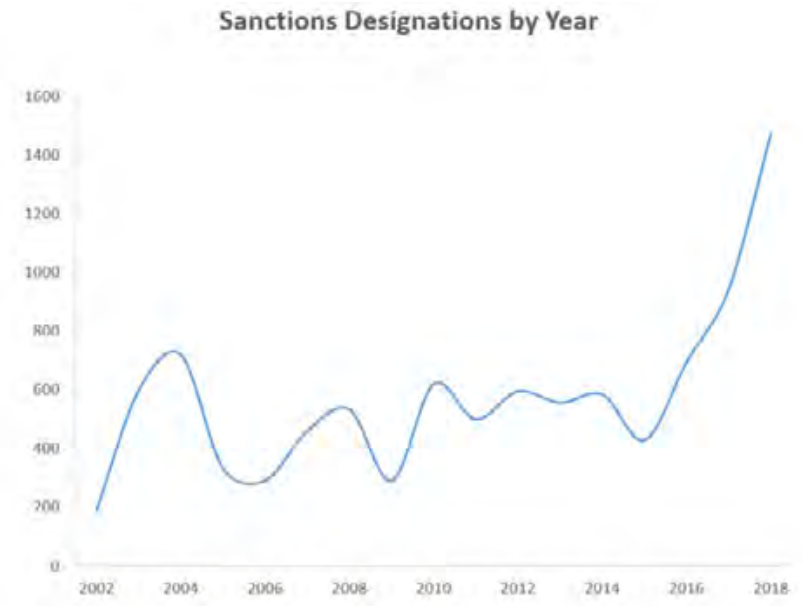
- 2018 was another notable year for U.S. sanctions:
  - ***Record Increase in Designations:*** The U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") designated a record 1,474 new entities.
  - ***Unilateral Enforcement:*** Many of these designations were a result of the re-imposition of sanctions on Iran after the United States unilaterally withdrew from the Joint Comprehensive Plan of Action ("JCPOA"). This decision created a policy divergence with European allies, which have implemented a blocking statute to prevent European companies from enforcing U.S. sanctions.
  - ***New Enforcement Mantra:*** OFAC is becoming more aggressive in how it enforces sanctions violations by requiring companies to undertake compliance obligations as part of a resolution beyond paying a fine.
  - ***Reaching Cryptocurrencies:*** The United States has taken a number of steps to enforce sanctions against cybercrime and digital currency transactions.

Sanctions
U.S. Update

- In 2018, OFAC issued only seven civil penalties. But it would be a mistake to equate that number to a slowdown in sanctions enforcement, for multiple reasons:

  – ***New Designations:*** OFAC's designation of 1,474 new entities was a **60% increase** over **any** prior year.

  – ***Massive Fines Continue:*** In November, Société Générale S.A. ("SocGen") entered into a resolution with several U.S. regulators, including OFAC, to resolve allegations of sanctions violations. SocGen paid **$1.34 billion**, the second-largest penalty against a financial institution for sanctions violations in history.



  - Notably, in a departure from prior practice, OFAC **did not credit** SocGen's payments to other regulators. This may reflect part of OFAC's new enforcement mantra.

Iran Sanctions Program

Key Developments

- ***Withdrawal:*** On May 8, President Trump announced his decision to unilaterally withdraw from the 2015 JCPOA and re-impose U.S. nuclear-related sanctions on the Iranian regime.
- ***Re-Imposition:*** On November 5, after two wind-down periods, the United States re-imposed sanctions on Iran. That day, OFAC added more than 700 parties to the Specially Designated Nationals ("SDN") list—the most in a single day, ever. The United States has re-imposed sanctions on:
  - –Iran's energy sector;
  - –Petroleum-related transactions;
  - –Iranian port operators, shipping, and shipbuilding;
  - –Transactions by foreign financial institutions with designated Iranian financial institutions;
  - –Provision of specialized financial messaging services for certain Iranian financial institutions; and
  - –Underwriting services, insurance, and reinsurance.

- ***Secondary Sanctions:*** The United States may now (again) also impose various secondary sanctions on certain non-U.S. persons.
- ***Oil Waivers:*** The United States granted waivers to eight countries—China, Greece, India, Italy, Japan, South Korea, Taiwan, and Turkey—to allow them to continue to import Iranian oil for six months. What will happen in May 2019?

Iran Sanctions Program

EU Blocking Statute

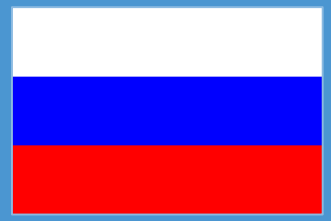
- In August, the European Union amended Council Regulation 2271/96, the "EU Blocking Statute." As amended, the EU Blocking Statute:
  - –Prohibits EU Operators from complying with U.S. sanctions on Iran imposed following the U.S. withdrawal from the JCPOA (*e.g.*, termination of ongoing business solely due to U.S. sanctions pressure). EU Operators risk criminal and administrative fines for violations;
  - –Allows EU Operators to cease business operations in Iran, and to decide whether to engage or not in an economic sector on the basis of their assessment of the economic situation;
  - –Allows EU Operators to recover "any damages, including legal costs," caused by the application of the re-imposed U.S. sanctions on Iran—thus increasing litigation risk for counterparties that seize business solely due to the re-imposed U.S. sanctions on Iran; and
  - –Requires EU Operators to report to the EU if they are affected by re-imposed U.S. sanctions on Iran.

Bottom Line

- To date, the dominance of the U.S. dollar, together with robust U.S. sanctions enforcement, forces many global firms to comply with the re-imposed U.S. sanctions, even in light of legal risks arising from the EU Blocking Statute and other national anti-boycott legislation.
- We can expect more appetite for enforcement of the EU Blocking Statute and similar laws in European countries given widespread objections to the foreign policies of the Trump Administration.
- We also can expect litigation against parties that decide to comply with the re-imposed U.S. sanctions.

Russia Sanctions Program

Key Developments



- On April 6, OFAC announced 38 new designations pursuant to existing sanctions programs, including six oligarchs (one of whom was Oleg Deripaska), 12 oligarch-owned or controlled businesses, 17 senior Russian government officials, and two Russian state-owned companies.
- ***Russian Sanctions:*** In June, Russia passed a law authorizing the government to implement counter-sanctions against "unamicable foreign states," including:
  - –Termination of cooperation;
  - –An import and export ban; and
  - –Any other retaliatory measures.
- ***Delisting Debate:*** After the April 6 sanctions, Deripaska substantially decreased his ownership in three designated companies (EN+ Group plc, United Company RUSAL and SC EuroSibEnergo).
  - –On January 27, 2019, these three companies were delisted.
  - –Oleg Deripaska himself remains listed as an SDN.

Effects of the April 6, 2018 Designations

- Dramatic fall in Russian stocks;
- The ruble fell nearly 5% against the U.S. dollar; and
- RUSAL's share price on the Hong Kong stock exchange fell 50% the day after the sanctions were announced.

RTS Index

Venezuela Sanctions Program

Key Developments

- Since 2018, the United States has imposed a number of new sanctions to address the deteriorating political and economic situation in Venezuela.
- ***2018 Sanctions:*** In 2018, the United States issued sanctions targeting:
  - –Dealings in or related to any digital currency sponsored by the Venezuelan government;
  - –U.S. persons engaging in certain dealing of debt or equity owed to the Government of Venezuela; and
  - –Venezuela's gold sector and corruption in its government.
- ***2019 Sanctions – Designation of PdVSA:*** On January 28, 2019, OFAC designated Petróleos de Venezuela, S.A. ("PdVSA") as an SDN.
  - –PdVSA is one of the largest companies OFAC has even sanctioned.
  - –PdVSA is more linked to U.S. interests than almost any prior designation. (PdVSA sells the United States 500,000 barrels of day of oil, owns refineries, and employs thousands of Americans.)
  - –OFAC issued 8 general licenses in tandem with the designation, continuing a trend of issuing broad sanctions that are calibrated through the issuance of general licenses.
  - –There likely will be more FAQs released given the complexity of this action.

> *"'[The] designation of PdVSA will help prevent further diverting of Venezuela's assets by Maduro and preserve these assets for the people of Venezuela."*
>
> – Steven T. Mnuchin, Secretary of the Treasury, January 28, 2019

Sanctions Program

Areas of Innovation – Digital Currencies and Election Interference

- OFAC continues to apply sanctions in innovative ways, including against cryptocurrency transactions and interference in U.S. elections.
- On March 19 and June 6, OFAC issued guidance clarifying the application of U.S. sanctions to cryptocurrency.
- On November 28, OFAC designated two Iranian individuals who helped cybercriminals exchange bitcoin they received as ransom into Iranian rials. The OFAC designations included their digital currency addresses:

The following individuals have been added to OFAC's SDN List:

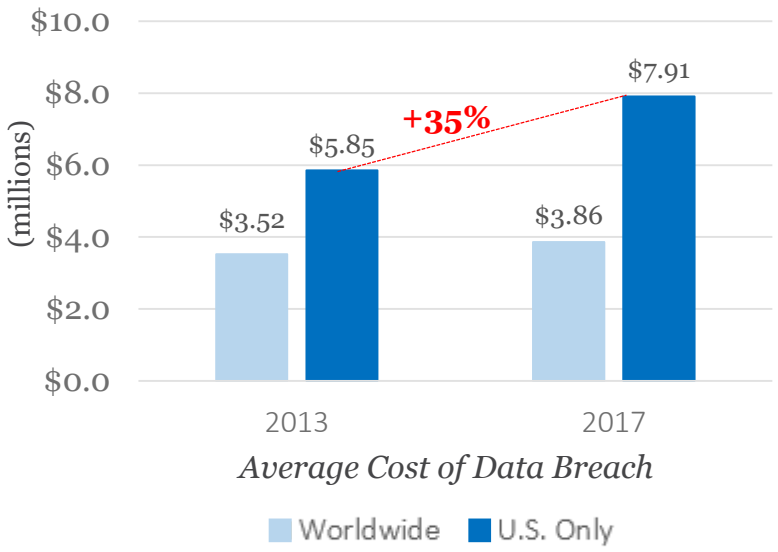
GHORBANIYAN, Mohammad (a.k.a. GHORBANIAN, Mohammad; a.k.a. "EnExchanger"; a.k.a. "Ensaniyat"; a.k.a. "Ensaniyat_Exchanger"), Iran; DOB 09 Mar 1987; POB Tehran, Iran; nationality Iran; Website www.enexchanger.com; Email Address EnExchanger@gmail.com; alt. Email Address Ensaniyat1365@gmail.com; Additional Sanctions Information - Subject to Secondary Sanctions; Gender Male; Digital Currency Address - XBT 1AjZPMsnmpdK2Rv9KQNfMurTXinscVro9V; Identification Number 008-046347-9 (Iran); Birth Certificate Number 32270 (Iran) (individual) [CYBER2].

- In September, President Trump signed an executive order that targets interference in U.S. elections with the threat of sanctions. These sanctions are not limited to Russian interference. As Director of National Intelligence Daniel Coats stated, "[i]t is more than Russia here that we are looking at."

Data Privacy and Security
Threats and Trends

- Many data breaches start with mistakes:
  - –The New York Attorney General attributed a quarter of 2017 breaches to negligence, including inadvertent disclosure and lost devices.
  - –An SEC investigation in October found that nine public companies lost almost $100 million from cyber frauds where employees wired money to individuals posing as executives or vendors.
- Ransomware epidemic:
  - –Ransomware accounted for almost half of all malicious software in 2017, and can lead to financial consequences from damaged business operations as well as extorted payoffs.
  - –Approximately 93% of malware, including ransomware, is spread via e-mail—underscoring the importance of anti-phishing training.

U.S. Data Breach Costs Rose Faster than the Global Average from 2013 to 2017



Data compiled from Ponemon Institute - 2018 Cost of Data Breach Study and Ponemon Institute - 2015 Cost of Data Breach Study

Data Privacy and Security
Litigation Developments

- Plaintiffs continued to respond to cyber incidents with securities litigation in 2018.
  - –Five derivative lawsuits naming directors and officers related to data breaches were filed in 2018, and two were filed in 2017. Prior to 2017, the cumulative total was six.
  - –Companies continue to pay significant monies to resolve these matters. For example, in July, GameStop agreed to pay up to ~$305.5 million in customer reimbursements (up to $235 per card for approximately 1.3 million credit and debit cards); up to $10,000 per plaintiff for "extraordinary loss"; and $0.6 million in fees and costs.
- 2018 saw an executive charged with insider trading after participating in a company's data breach response.
  - –In a case related to the same breach, a software engineer who worked on the incident response pled guilty to insider trading and was sentenced in October to house arrest.

Data Privacy and Security

Regulatory Developments

- Testifying before Congress in July, Federal Trade Commission ("FTC") Chairman Joseph Simons stated that "privacy and data security top the list" of the FTC's consumer protection priorities.
- The FTC continued its 2017 trend of requiring third-party security audits for up to 20 years in data breach settlements.
- The FTC emphasized its focus on individual accountability.
- September 2018 was the end of the inaugural year for the SEC's cyber enforcement unit, with enforcement efforts focused on:
  - Allegations of using hacked information to gain an improper advantage;
  - Misconduct related to cryptocurrency; and
  - Public company disclosures of cybersecurity risks and incidents.

"I believe the FTC should hold individual executives accountable . . . [T]his relief is important, because it ensures that individual executives who control the operation of the firm—and not just shareholders—bear the costs of noncompliance."

– Rohit Chopra,
FTC Commissioner,
May 14, 2018

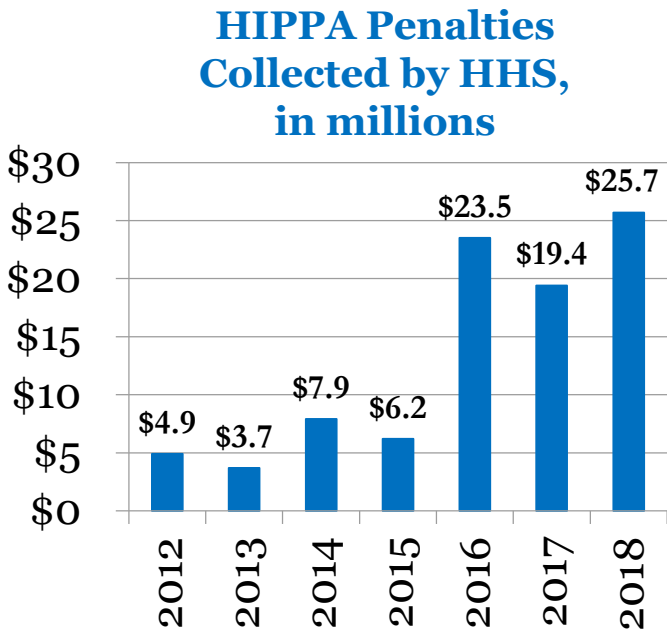
"The Commission's latest guidance . . . relies heavily on the judgments of corporate counsel to make sure investors get the information they need. I worry that these judgments have, too often, erred on the side of nondisclosure."

– Robert J. Jackson, Jr., SEC Commissioner,
Mar. 15, 2018

Data Privacy and Security

Regulatory Developments

- Federal regulators and state AGs vigorously pursued actions under the Health Insurance Portability and Accountability Act ("HIPPA") related to cybersecurity incidents in 2018.
  - –The U.S. Department of Health and Human Services ("HHS") collected more than $20 million in data-breach-related HIPPA fines in 2018, including $16 million for the largest HIPPA settlement in history.
  - –The first ever HIPPA-related data breach case involving multiple state AGs was filed in 2018.
- In December, HHS issued voluntary cybersecurity guidelines with the goal of "rais[ing] the cybersecurity floor across the health care industry." HHS described the risks and offered risk-minimization suggestions for five prevalent threats:
  1) E-mail phishing attacks;
  2) Ransomware attacks;
  3) Loss or theft of equipment or data;
  4) Insider, accidental or intentional data loss; and
  5) Attacks against connected medical devices that may affect patient safety.



Data Privacy and Security

UK and European Developments

- The General Data Protection Regulation ("GDPR") entered into force on May 25, 2018.
  - National data protection authorities report a significant increase in data protection complaints since that date, including complaints lodged against technology companies by civil society groups.
- On January 22, 2019, the French data protection regulator, CNIL, imposed a €50 million financial penalty on Google for "lack of transparency, inadequate information and lack of valid consent regarding the ads personalization."
- Data protection authorities are scaling up their enforcement capability. For example, the UK Information Commissioner's Office ("ICO") is increasing staff from 442 in 2016 to 537 in 2018, and Germany's data protection office has hired more than 400 people.
- The ICO announced an investigation into reported data breaches at British Airways.
- On December 19, the European Commission ("EC") published a report on the second annual review of the functioning of the EU-U.S. Privacy Shield. The EC found that "the U.S. continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield"; nomination of a permanent Ombudsman is expected by February 28, 2019.
- Companies should be conscious of the impact of GDPR as they carry out internal investigations, particularly with respect to data collection, processing, and production.

Bank Secrecy Act/Anti-Money Laundering

Key Trends and Developments

- 2018 has seen several large BSA/AML enforcement actions, reflecting heightened risks for financial institutions.
  - –There were four resolutions of more than $100 million in 2018.
- In 2017 and 2018 remarks, Deputy Attorney General Rosenstein stressed that prosecutors would pursue AML enforcement with vigor and increased sophistication.
- Enforcement actions are becoming increasingly complex, often involving multiple regulators and, at times, multiple jurisdictions.
- Foreign regulators are pursuing increasingly robust AML/CTF actions, such as a $900 million resolution in the Netherlands and a $700 million resolution with Australia's largest bank.
- Prosecutors are increasingly targeting failure to file SARs.

Key Trends in BSA/AML Enforcement

- Increased prosecutorial focus
- Multiple actors: federal, state, and foreign
- Government coordination of enforcement actions
- Increasing compliance obligations
- Growing emphasis on voluntary self-disclosure
- Focus on individual accountability
- Convergence with cybersecurity
- De-risking as priority

Bank Secrecy Act/Anti-Money Laundering

Key Enforcement Agencies

- New York's DFS continued to be an active state regulator in 2018:
  - –Three AML consent orders imposed a total of $195 million in fines. Two of the three agreements followed the imposition of related fines by federal regulators; the third, a $40 million fine imposed on a UAE financial institution and its New York branch, had no related federal resolution.
  - –Linda Lacewell was nominated for DFS Superintendent to replace Maria Vullo, who is stepping down effective Feb. 1, 2019.
- In its 2018 priorities letter, BSA/AML compliance remains a focus area for the Financial Industry Regulatory Authority ("FINRA"), which entered into ten resolutions in 2018, three with individual employees or representatives of regulated financial institutions. FINRA singled out the use of foreign affiliates as an area of concern.
- The Office of the Comptroller of the Currency ("OCC") conducted 17 enforcement actions with financial institutions in 2018, including a standalone $100 million resolution for a U.S. bank's violations of a prior consent order.
- FinCEN brought fewer enforcement actions than in years past, but remains actively involved in regulating and monitoring transactions in the BSA/AML space.

Bank Secrecy Act/Anti-Money Laundering

Key Developments in Criminal Enforcement

- DOJ concluded five criminal BSA/AML resolutions in 2018, three of which featured total settlement amounts of more than $100 million. Notable resolutions include:
  - In February, a U.S. subsidiary of a Dutch bank entered into a $368 million plea agreement and admitted that deficiencies in its BSA/AML compliance program facilitated cash-based transactions worth hundreds of millions of dollars from Mexico and elsewhere. The bank was also cited for obstructing an OCC examination.
  - Also in February, an American financial institution agreed to a $528 million resolution based on its failure to establish an adequate AML program; it paid $75 million as a fine to the OCC, with the remainder subject to civil forfeiture.
    - Initial investigation into suspicious activity of bank customer Scott Tucker led to broader evaluation and censure of the bank's compliance program.

  - In March, a Texas gold refinery agreed to forfeit $15 million for AML violations relating to its failure to adequately monitor the provenance of gold it accepted.
  - In November, DOJ extended a 2012 DPA with a money-services business for an additional 30 months and imposed an additional $125 million fine based on a finding that the company's BSA/AML compliance controls remained inadequate.

Bank Secrecy Act/Anti-Money Laundering

Key Regulatory and Legislative Developments

- FinCEN issued its second set of FAQs regarding new Customer Due Diligence ("CDD") requirements that went into effect on May 11, 2018.
- FinCEN issued in June a new advisory highlighting the connection between foreign corruption and human rights abuses, warning regulated financial institutions to be wary of efforts to conceal the proceeds of political corruption and to promptly and thoroughly report suspicious activities.

- There continues to be significant legislative attention to reforming and updating the BSA, with multiple bills introduced in 2018 and another one already introduced earlier this month.
- The Federal Reserve Board ("FRB"), Federal Deposit Insurance Corporation ("FDIC"), FinCEN, National Credit Union Administration ("NCUA"), and OCC issued a joint statement in October regarding how smaller financial institutions may collaborate and share resources to more efficiently satisfy their BSA/AML obligations.
- FinCEN released an advisory in connection with the United States' withdrawal from the Iran nuclear deal and consequent re-imposition of sanctions advising financial institutions to be mindful of their obligations under OFAC sanctions.

AML

United Kingdom and European Union Update

United Kingdom

- January saw the establishment of the Office for Professional Body Anti-Money Laundering Supervision ("OPBAS") to strengthen defenses against money laundering and terrorist financing.
- In May, the UK Sanctions and Anti-Money Laundering Act received Royal Assent for the UK to impose economic and other sanctions, and money laundering and terrorist financing regulations, after Brexit.
- In October, the UK High Court dismissed the first challenge to an Unexplained Wealth Order ("UWO").
- The Financial Action Task Force ("FATF") conducted an assessment and published a report in December concluding that, while the UK AML and counter-terrorist financing regime is effective in many respects, it is weak in areas such as supervision and the reporting and investigation of suspicious transactions.
  - In July, the Law Commission published a consultation paper regarding the current SAR framework. Issues identified include voluminous disclosures, poor quality of disclosures, and the overall burden of compliance on entities required to report suspicious activity.
  - The National Crime Agency's ("NCA") latest Annual Report states that the number of SARs received by the UK Financial Intelligence Unit ("UKFIU") increased by 10% compared to the previous year.

European Union

- The European Council adopted a fifth anti-money laundering directive in October, requiring implementation by January 10, 2020.

SEC Disclosure Practices

Trends and Developments

- ***Disclosures***
  - ***Board Diversity*:** A growing number of companies are voluntarily enhancing their disclosures to highlight the diversity of their boards.
  - ***Cybersecurity:*** Companies have been increasing their focus on cybersecurity disclosure in connection with both cybersecurity incidents and descriptions of board oversight and expertise.
- ***SEC Disclosure Update and Simplification:*** In August, the SEC adopted several dozen amendments to existing disclosure requirements "to simplify compliance without significantly altering the total mix of information"; the final rules are largely consistent with the changes proposed in 2016.

- ***Proposed Legislation to Expand Climate-Related Disclosures:*** In September, the Senate introduced the Climate Risk Disclosure Act of 2018, which would require public companies to disclose substantial new information about their exposure to climate-related risks; the disclosures would be intended to provide qualitative and quantitative information about financial risks from climate change and climate change mitigation.

Governance

2018 Proxy Season Update

- ***Fewer Proposals, but Higher Support*:** Shareholders submitted 788 proposals during the 2018 proxy season,* down 5% from the 827 proposals submitted during the 2017 proxy season and 14% from the 916 proposals submitted during the 2016 proxy season. The average support, however, increased by almost 4 percentage points.

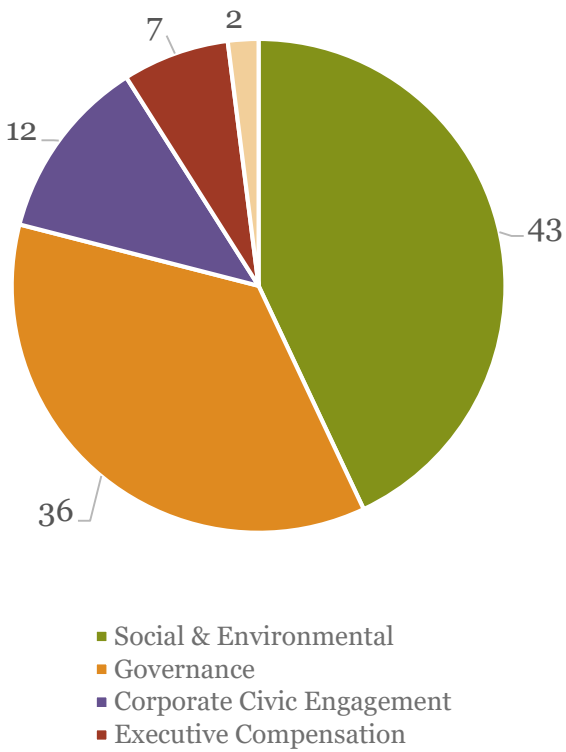
- ***Say-on-Pay Votes:*** According to ISS, the failure rate of say-on-pay proposals doubled to 2.5%, compared to 1.2% in 2017, with the most common reasons for low say-on-pay votes in 2018 to date lack of rigorous performance criteria and high levels of pay.

- ***Stockholder Proposals:***

  – Environmental, social, and governance ("ESG") issues continue to be the focus of stockholder proposals.

  – "Perennial topics" trending consistent with 2017 include political contributions and lobbying (11% of all proposals); climate change (9%); anti-discrimination and diversity (9%); independent chair (7%); and proxy access proposals replaced by special meeting proposals (10%).

Shareholder Proposals Submitted in 2018 Proxy Season (%)



* Statistics reflect voting results of Russell 3000 companies from January 1, 2018, through August 13, 2018.

Governance

New SEC Guidance Regarding Shareholder Proposals

- On October 23rd, the SEC's Division of Corporation Finance issued Staff Legal Bulletin 1 ("SLB 14J") explaining how and when board analyses can assist the Staff in its analysis of requests to exclude shareholder proposals on economic relevance or ordinary business grounds.
  - –SLB 14J also provides insight into the Staff's approach to the ordinary business arguments regarding micromanagement and proposals touching on senior executive and/or director compensation matters.
- During the government shutdown, the SEC was unable to respond to shareholder proposal exclusion no-action letter requests. The impact of any backlog created by the shutdown are yet to be determined.

Chairman Clayton noted that the Staff is reviewing ownership and resubmission thresholds for shareholder proposals, asking whether there are factors other than time/amount that *"reasonably demonstrate that the proposing shareholder's interests are aligned with those of a company's long-term investors."*

– Jay Clayton, SEC Chairman,
Dec. 6, 2018

Governance

Proxy Advisory Firm Updates

- ***Board Gender Diversity:*** ISS and Glass Lewis have adopted policies to recommend voting "against" nominating committee chairs of boards on which no female directors serve.
- ***Board Meeting Attendance:*** New ISS policy codifies approach on poor attendance at board meetings: when a director has "chronic poor attendance without reasonable justification," ISS will now recommend voting "against" appropriate members of the nominating/governance committees or the full board, in addition to voting "against" the offending director.
- ***Auditor Ratification Proposals:*** Glass Lewis policy codifies new factors to be considered for auditor ratification: auditor's tenure, a pattern of inaccurate audits, and any ongoing litigation or significant controversies that call into question an auditor's effectiveness.
- ***ESG Risk Oversight:*** Glass Lewis now may recommend voting "against" directors responsible for ESG risk oversight if a company does not properly manage those risks and it impacts shareholder value.
- ***Director Accountability for Management Proposals Used to Exclude Shareholder Proposals:*** ISS and Glass Lewis adopted policies to recommend voting "against" certain directors when a proxy statement includes a management proposal used to exclude a conflicting shareholder proposal on specified items.
- ***Virtual-Only Shareholder Meetings:*** Effective on January 1, 2019, Glass Lewis may recommend votes "against" the members of the nominating/governance committee if the company does not provide "effective" disclosure assuring that shareholders will have the same opportunities to participate at the virtual meeting as they would at in-person meetings.

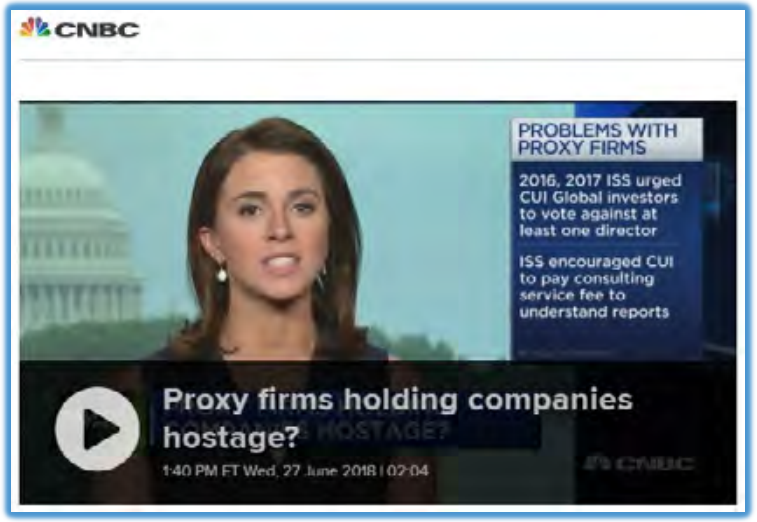
Governance

Proxy Advisory Firm Updates (cont'd)

- Increased focus on the regulation of proxy advisory firms in light of widespread criticism over their perceived undue influence has led to:

  –***Proposed Legislation:*** The Corporate Reform and Transparency Act would regulate the activities of proxy advisory firms by requiring registration with the SEC and requiring certain qualifications. The bill passed the House but has stalled in the Senate.

  –***No-Action Letters Withdrawn:*** In September, the SEC issued a public statement that it had withdrawn two no-action letters issued in 2004, which had been criticized as affirming the influence of proxy advisory firms by indicating that such firms could be considered "independent third parties" when issuing voting recommendations to investment advisers.



  –***Proxy Process on SEC Agenda:*** In December, Chairman Clayton said in a speech about SEC rulemaking that a "significant initiative for 2019 is improving the proxy process," including the need for "greater clarity" regarding the division of labor, responsibility, and authority between proxy advisory firms and the investment advisers they serve.

Governance

Increased Focus on ESG Issues and Ratings

- ***Increased Focus on ESG issues:*** Investors and stockholders increasingly focus on companies' ESG performance and disclosure, and often rely on third-party ESG reports and ratings.
- ***Delaware Certification of Company Sustainability Efforts:*** In June, Delaware adopted the Certification of Adoption of Transparency and Sustainability Standards Act, which creates an entirely voluntary process for certifying Delaware-law entities that adopt "sustainability standards" and "assessment measures."
- ***Liability Concerns and Board Oversight:*** Sustainability reports and other ESG-related communications are generally not audited by third-party consultants for accuracy or reviewed or approved by boards. Nonetheless, ESG disclosures, even when made outside of SEC filings, can give rise to liability under the securities laws: it is important that boards maintain awareness and oversight of these disclosures in light of rapidly expanding ESG disclosures and increased investor attention.

Governance
Board Diversity

- ***Progress on Board Diversity:*** Per ISS, the percentage of new directors who are female reached a record high of 35% in the Russell 3000 and almost 39% in the S&P 500, and approximately 90% of S&P 500 and 58% of Russell 3000 companies have at least two female directors.
  - –Nonetheless, 18% of Russell 3000 companies have no female directors.
- ***California Legislation:*** On September 30th, California Governor Jerry Brown signed SB 826 into law (effective January 1, 2019), requiring a minimum number of female directors on the boards of publicly traded corporations with principal executive offices in California.
  - –This may apply to 377 companies in California that will need to add female director(s). "Female" is defined as any person who self-identifies as a woman.
  - –Corporations must have at least one female member on their board of directors by December 31, 2019, and at least two female directors by 2021 for boards with five directors and three female directors for boards of six or more directors.
- ***Investor Developments:***
  - –State Street announced that, in 2020, it will begin voting against all nominating committee members of U.S., UK, and Australian portfolio company boards that do not have at least one woman and have not engaged in "successful dialogue" with SSGA on this topic for three consecutive years.
  - –For annual meetings on or after February 1, 2020, ISS generally will vote "against" or "withhold" from the nominating committee chairs of public companies without women on their boards.
  - –For annual meetings after January 1, 2019, Glass Lewis will begin recommending votes against the nominating committee chair of company boards with no female directors. Votes against other committee members may also be recommended, depending on various factors.

Governance

Cybersecurity Developments and Board Oversight

- ***SEC guidance:*** February 2018 SEC guidance on cybersecurity disclosures emphasized:
  - ***Board Oversight:*** The board's role in overseeing risks should be disclosed if "cybersecurity risks are material to a company's business"; disclosure should also show how the board engages with management on cyber issues.
  - ***Criteria for Determining Materiality:*** Certain criteria that companies should consider include the nature/magnitude of a cyber risk or incident; reputational, financial or operational harm; and potential litigation/regulatory actions.
  - ***Timing of Disclosures:*** An internal or external investigation would not on its own provide a basis for avoiding disclosure of a material cyber incident.
  - ***Insider Trading:*** Companies are encouraged to consider how their code of ethics and insider trading policies take into account and prevent insider trading on the basis of material non-public information related to cybersecurity risks and incidents.
  - ***Policies and Procedures:*** Companies are encouraged to have comprehensive policies (*e.g.*, disclosure and risk management policies and procedures) to cover cybersecurity issues (*i.e.*, to enable companies to identify and elevate information promptly so appropriate disclosure can be made in a timely manner).

Governance

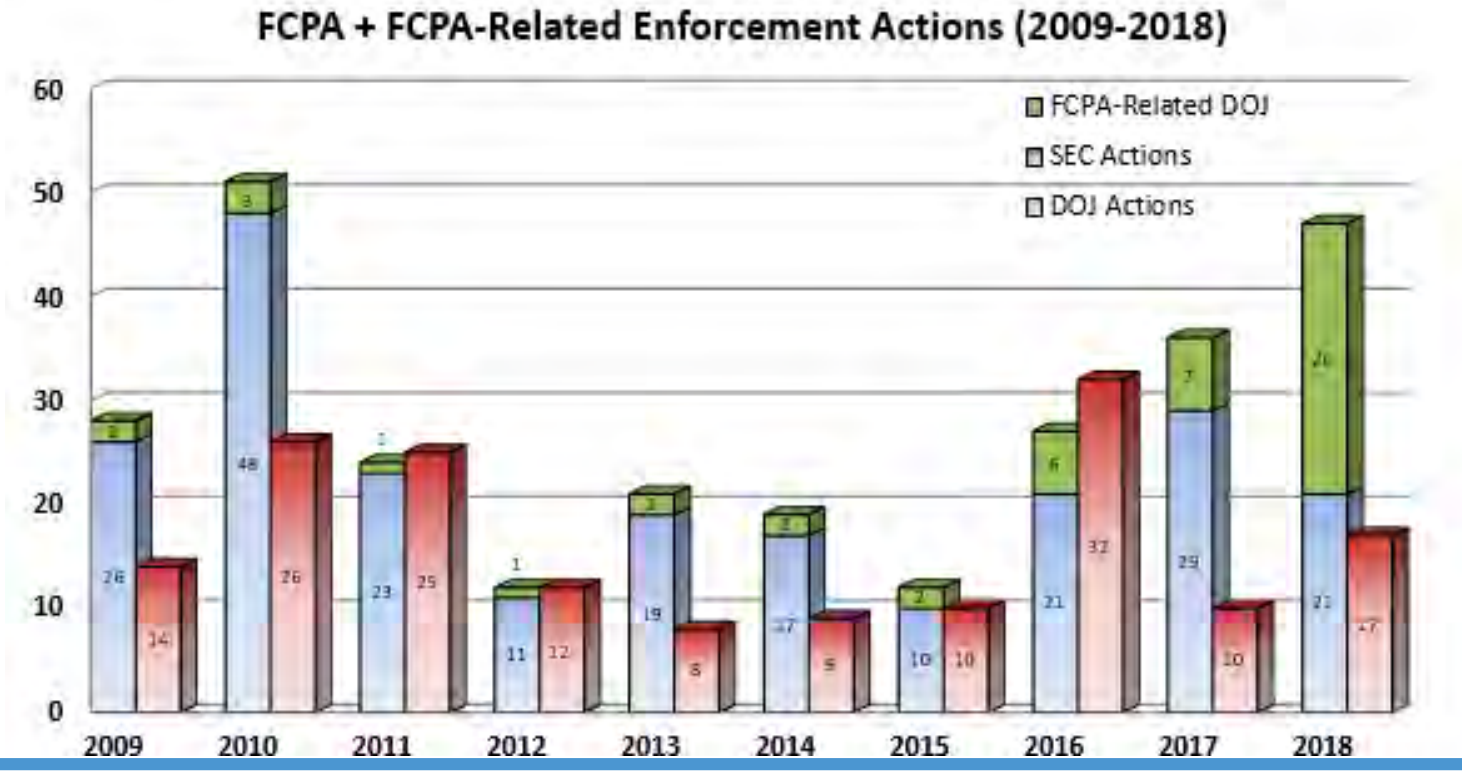
Board Oversight in the #metoo Era

- ***Board Oversight of Anti-Harassment Programs and #metoo Issues:***
  - 2018 has seen an increased focus on the adoption of anti-harassment policies and programs.
    - Since October, for example, New York State's sexual harassment policy has required companies to adopt the state's model policy, at a minimum.
  - There also has been an increased focus on board oversight of anti-harassment programs and reporting mechanisms in light of widely publicized corporate investigations, scandals, and settlements involving allegations of inadequate oversight.
    - This focus raises questions regarding the scope of the board/committee oversight function. For example, should board oversight be limited to complaints against upper management or to compliance and reporting programs more generally?
- ***Corporate Culture and Labor Issues:***
  - Sexual harassment scandals have triggered increased discussion regarding the importance of corporate culture and board oversight thereof, particularly workplace bullying, workplace safety and labor conditions, and work/life balance.
  - Sexual harassment issues have been linked to increased controversy regarding the use of mandatory arbitration and non-disclosure agreements and other restrictive labor arrangements.

White Collar and Securities Fraud

FCPA Enforcement by the Numbers

- FCPA enforcement in 2018 was on par with previous years, although the number of pure FCPA enforcement actions was down moderately from the previous two years.
- When pure FCPA resolutions are combined with FCPA-related enforcement actions, such as money laundering charges against foreign official bribe recipients, 2018 becomes the second-most prolific year in the history of foreign anti-corruption enforcement by the U.S. government.



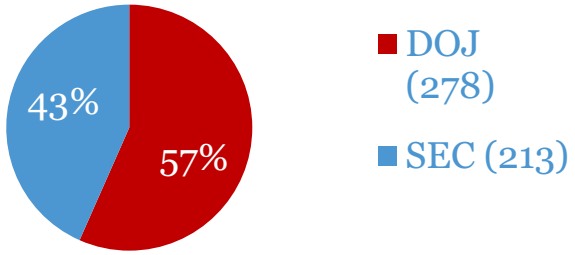
White Collar and Securities Fraud

DOJ and SEC FCPA Enforcement

- SEC enforcement continued along historical averages, with 17 FCPA actions in 2018. DOJ enforcement was down slightly from 2017, with 21 pure FCPA actions in 2018.
- In May, DOJ introduced a new "Policy on Coordination of Corporate Resolution Penalties," attempting to discourage "piling on" by different enforcement authorities punishing the same company for the same conduct. The policy largely reflects pre-existing DOJ practice in the FCPA space.
- On August 24, the Second Circuit held in *United States v. Hoskins* that a foreign national who does not otherwise fall under "the categories of persons directly covered" by the FCPA cannot be held liable for violating the statute under conspiracy liability theories.

> *"[A]dopting the government's view that the jurisdictional reach of the FCPA must be coterminous with that of bribery . . . would transform the FCPA into a law that purports to rule the world."*
>
> – Judge Pooler, Second Circuit, *U.S. v. Hoskins*

491 Total FCPA Enforcement Actions: 2005 - 2018



- The Operation Car Wash-related resolutions, including the September Petrobras resolution, highlight the continued global coordination of FCPA enforcement actions.

White Collar and Securities Fraud

United Kingdom Update

- Lisa Osofsky is the new Director of the Serious Fraud Office ("SFO").
- The SFO is actively engaged in a number of cross-border investigations, including a cluster of investigations related to the use of Unaoil (Monaco) S.A.M. by companies in the oil and gas sector.
- In September, the English Court of Appeal reversed the High Court's decision in *SFO v. ENRC,* clarifying English law regarding litigation privilege in connection with internal investigations.

- No DPAs were concluded in 2018.
- In 2018, six individuals were convicted of bribery or corruption offenses, and 12 individuals were convicted of fraud offenses, in SFO trials in the UK, with custodial sentences ranging up to eight years.
- 11 individuals were acquitted* in SFO trials (including two Tesco directors in a trial over a £250 million accounting irregularity).
- Multiple UK agencies are developing the National Economic Crime Centre ("NECC"), a body that is meant to plan, task, and coordinate inter-agency operational responses to centralize and improve the UK's capabilities to tackle economic crime.

* Or otherwise not found guilty (*e.g.*, because the Court ruled that there was no case to answer against them).

White Collar and Securities Fraud

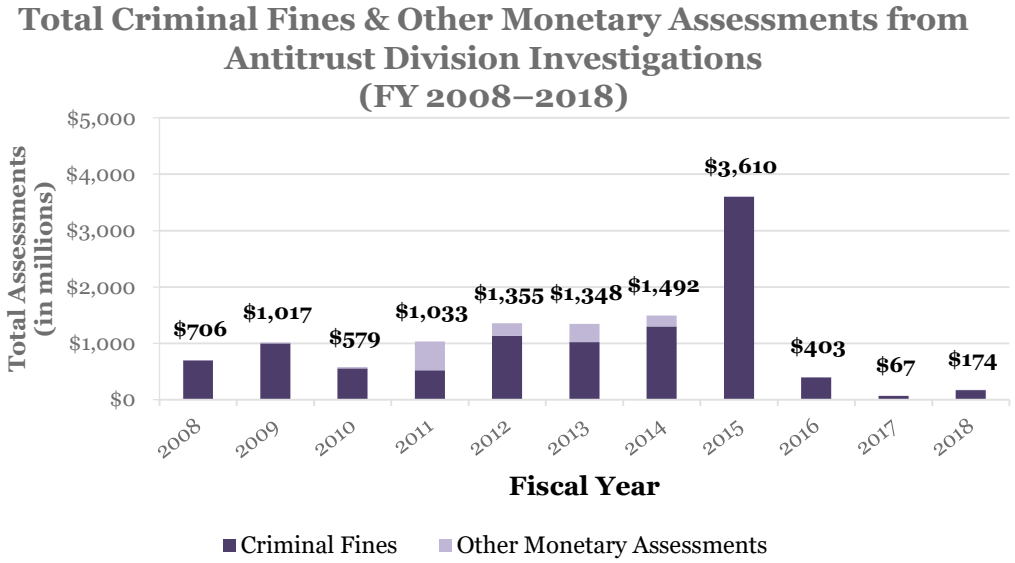
Criminal Export Control Developments

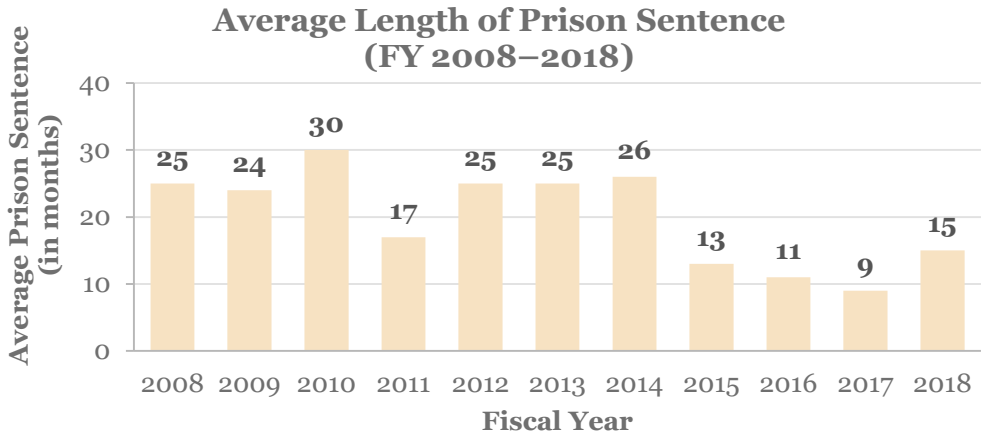
- As part of its China Initiative, DOJ unsealed charges against several Chinese and Taiwanese companies and individuals for trying to steal trade secrets from Micron, a semiconductor company.
- ***Emerging Technologies:***
  - In November, the Commerce Department's Bureau of Industry and Security published a request for the public's assistance in identifying "emerging technologies" essential for U.S. national security that should be subject to new export restrictions. These technologies include:
    - Biotechnology;
    - Artificial intelligence;
    - Additive manufacturing (*e.g.*, 3D printing);
    - Robotics; and
    - Advanced surveillance technologies.

Antitrust

U.S. Update – Criminal Enforcement

- DOJ filed 17 new criminal antitrust cases, continuing a downward trend that began in FY 2016.
- Several longstanding investigations (including auto parts; roll-on, roll-off shipping; and capacitors) appear to be winding down, compared to more robust activity in previous years.
- In congressional testimony, Assistant Attorney General Makan Delrahim, head of DOJ's Antitrust Division, identified areas of future investigative interest:
  - Online platforms with significant market power, including dominant entities leveraging users' personal information to stymie entry or growth by competitors.
  - Agreements between competitors not to hire or solicit each other's employees ("no-poach" agreements).
    - Assistant Attorney General Delrahim specifically mentioned that DOJ is including screening for this behavior during merger investigations.





Antitrust

U.S. Update – Policy Changes and Trends

- In FY 2018, DOJ Antitrust announced it would make consent decrees "more enforceable, less regulatory." The Division took several concrete steps towards this goal, including:
  - Creating an Office of Decree Enforcement tasked with ensuring consent decree compliance;
  - Changing its standard consent decree terms to reduce the burden of proof required for DOJ to establish a consent decree violation in court;
  - Seeking structural relief instead of regulatory behavioral conditions in consent decrees to remedy anticompetitive mergers; and
  - Beginning a systemic review and termination of "legacy" antitrust judgments that were entered into without a termination date.
- Assistant Attorney General Delrahim announced in September that he intends to "modernize" the merger review process.
  - Delrahim committed that DOJ would reduce its timeframe for reviewing mergers to six months in most instances. This would be a significant improvement over nearly 11 months for the average merger review in 2017.
  - In addition, DOJ will attempt to close merger investigations without requests for additional information ("Second Requests"), and issued clearer guidelines on the appropriate number of custodians and depositions necessary for merger review.

"I am deeply skeptical that Congress . . . envisioned a regime in which the Antitrust Division or a federal court would become the overseer of a company with thousands of employees, earning billions of dollars in annual revenues, and second-guessing market competition or future consumer or business behavior. In Section 7, Congress did not call for illegal mergers to be regulated, it called for them to be prohibited."

–Makan Delrahim, Assistant Attorney General, Apr. 26, 2018

Antitrust
United Kingdom Update

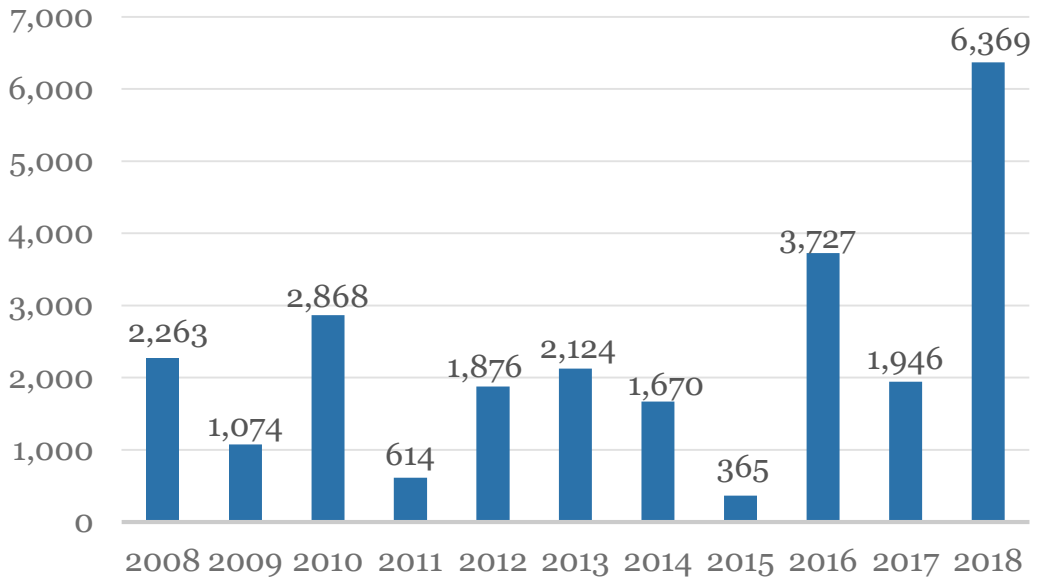
- UK and EU antitrust enforcers have continued to open new investigations in a number of industries and bring enforcement actions.
- The Competition and Markets Authority ("CMA") imposed fines against companies for conduct including participation in cartels (£3.4 million for bagged household fuel suppliers) and restricting competition (£1.6 million for Heathrow airport).
- Following the identification of a number of competition-related issues, the CMA announced a range of reforms related to the investment consultancy and fiduciary management sector.
- In October, the CMA announced the launch of a market study into the audit sector (specifically, the "Big Four" accounting firms) to examine "whether it is competitive and resilient enough to maintain high quality standards." The CMA has invited "interested parties" to comment on various issues.

- Pharmaceutical company Pfizer successfully appealed an £84.2 million fine imposed by the CMA in 2016 for excessive pricing of an anti-epilepsy drug.

Antitrust
European Union Update

- Record fines imposed by the European Commission ("EC").
  - –The EC fined Google €4.34 billion for alleged illegal practices, which the EC claimed were aimed at strengthening the dominance of Google's search engine.
  - –The EC issued fines totaling more than €111 million against four consumer electronics manufacturers for breaching EU competition rules by allegedly imposing fixed or minimum resale prices on their online retailers.

Fines Levied by the European Commission (€ in millions) 2008 – 2018



Calculation of EU Antitrust Fines

Starting point: Percentage (between 0% and 30% based on seriousness of the infringement) of company's annual sales of product concerned by the infringement, multiplied by the number of years of the infringement.

Adjustments: This is adjusted for aggravating and mitigating factors, and deterrence; possibility for fine to be decreased for leniency, settlement, and inability to pay.

Overall cap: 10% of total sales in the preceding business year.

Antitrust
Latin America & APAC Update

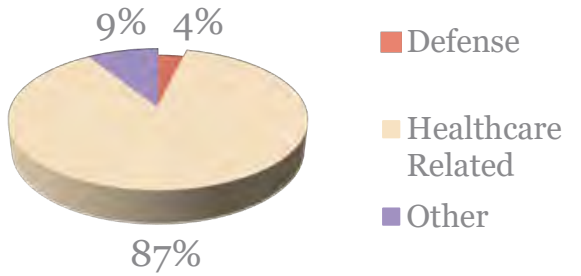
- ***Latin America:***
  - –In May, Argentina adopted a new law overhauling its competition law regime; the country is expected to establish a new antitrust authority by July 2019.
  - –In October, Brazil's antitrust authority issued guidelines on antitrust remedies. It also issued fines totaling $78 million against two dozen companies and trade associations for participating in a 20-year cartel in the country's salt market.
  - –In December, the competition authorities of Argentina, Brazil, Chile, Mexico, and Peru signed a joint statement on shared principles to guide the implementation of their leniency regimes and further reinforce their cooperation as part of the Latin American Strategic Alliance on Competition, formed in March 2017.

- ***Asia-Pacific:***
  - –Japan's antitrust authority announced plans to establish an organization to monitor the business practices of major tech firms amid growing concerns of market abuse.
  - –Australia's competition watchdog issued a preliminary report recommending improved oversight of tech giants and recommending that they be prevented from engaging in potentially discriminatory conduct.

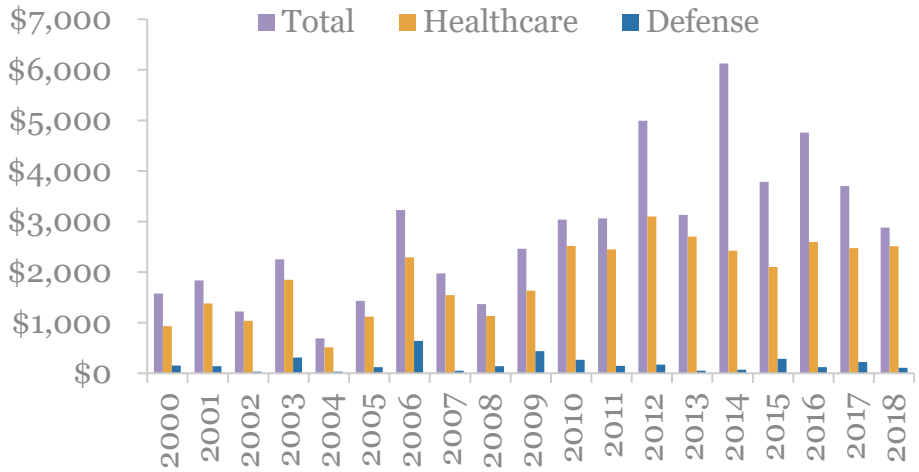
False Claims Act

- False Claims Act ("FCA") recoveries in 2018 fell below $3 billion for the first time in eight years; DOJ recovered $2.88 billion, down from $3.47 billion in 2017.
- Companies in the healthcare industry continued to dominate FCA investigations and enforcement actions, with over $2.5 billion in recoveries—up slightly from the previous year.
- DOJ's internal guidance memos and Supreme Court filing in *Gilead* signal a less expansive approach to FCA enforcement, especially in cases initiated by *qui tam* whistleblowers.
- Federal legislative and regulatory activity remained quiet; a recent decision by a district court in Texas striking down the Affordable Care Act ("ACA") in its entirety could negate the ACA's amendments to the FCA.
- State legislative activity continued during a "grace period" for states to increase civil penalties to match federal law and receive a 10% increase in the share of recoveries.

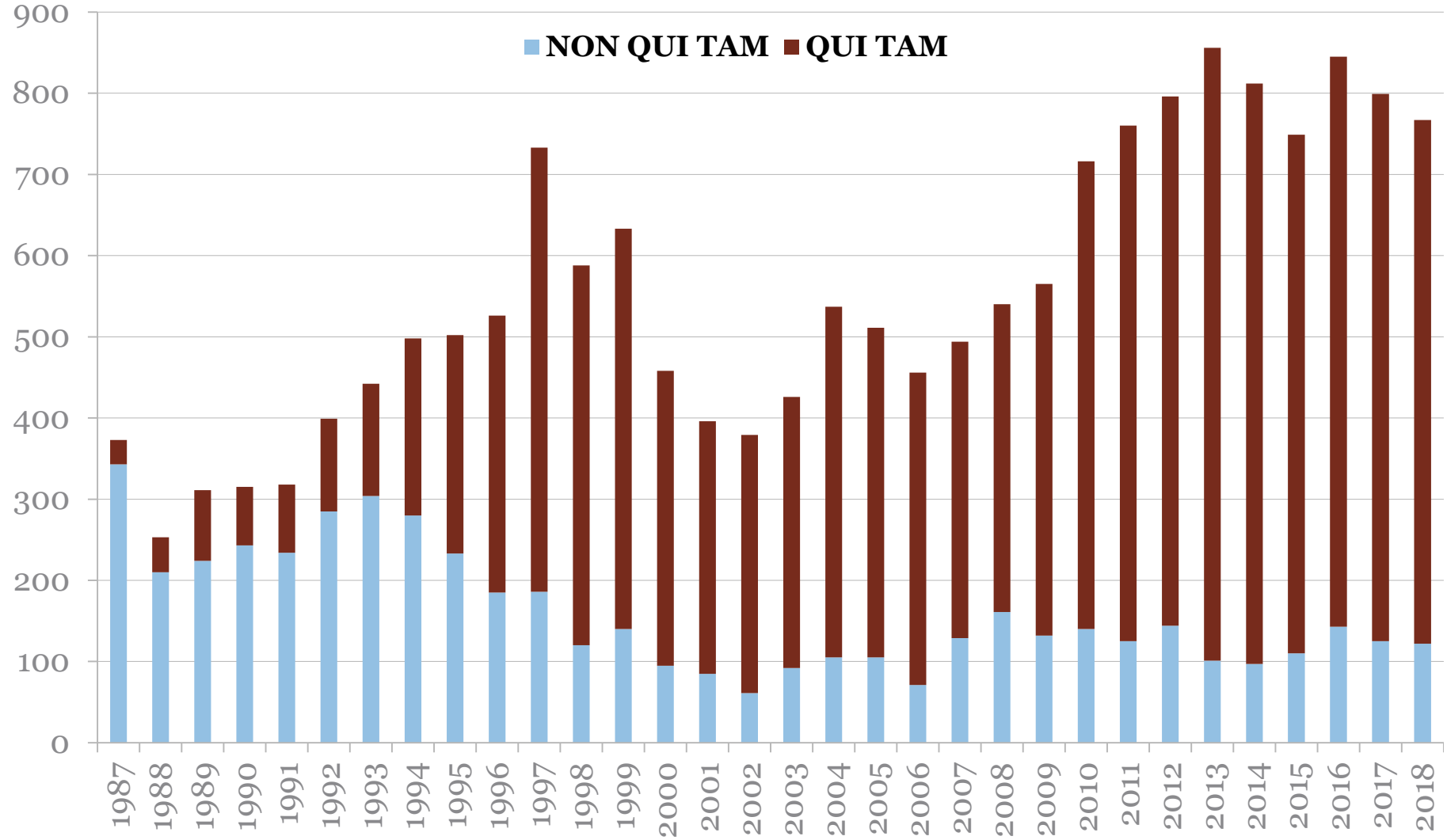
FCA Recoveries from the Defense and Healthcare Industries



Annual FCA Recoveries by Industry



False Claims Act Annual New Matters (1987 – 2018)



False Claims Act Post-*Escobar*

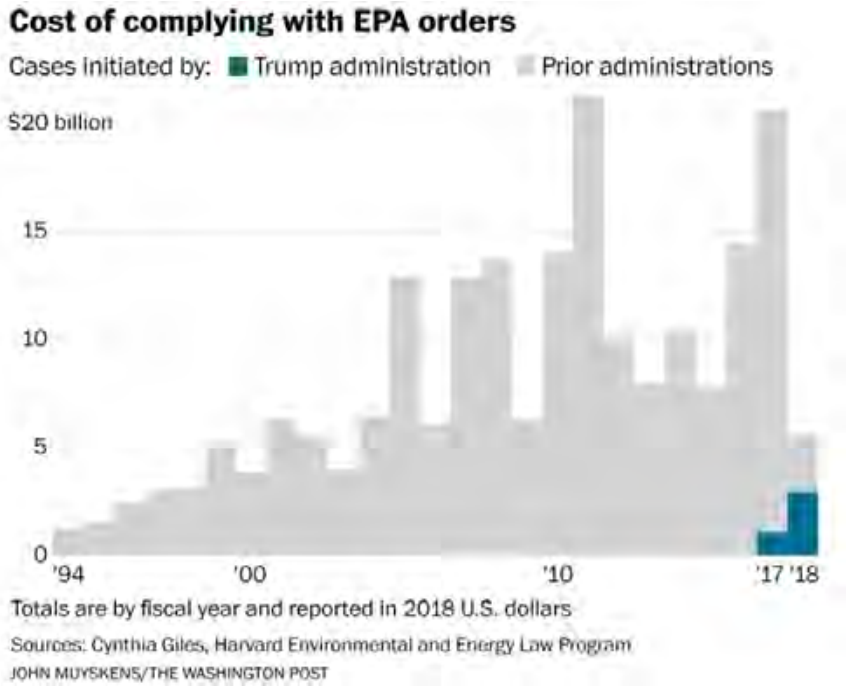
- In 2018, more than two years post-*Escobar*, appellate courts continued to debate the case's meaning.
  - –*Escobar* instructed courts to apply a "rigorous" and "demanding" materiality standard, necessitating a showing that the government actually refused payment, or would have refused payment, had it known of the alleged misrepresentations regarding compliance.
  - –The circuit courts have split on various issues, including:
    - When a claim for payment constitutes an implied certification of compliance with a regulatory or contractual obligation; and
    - What establishes or disproves the materiality of an allegedly false representation.
- In the January 2018 "Granston memo," DOJ signaled a willingness to use its dismissal authority to end FCA cases in certain situations, including when allegations are weak.
  - –In its amicus brief in *Gilead*, DOJ maintained its position on materiality post-*Escobar*, but indicated that, if the Supreme Court were to remand the case, DOJ would seek to dismiss it as "not in the public interest."
  - –DOJ cited "burdensome discovery" on the Food and Drug Administration as its main justification for seeking to dismiss *Gilead*, in line with the Granston memo's push to "preserve limited resources."

False Claims Act
Notable Judgments

- On January 11, 2018, a federal district court in Florida reversed a $350 million FCA jury verdict that a nursing home operator had submitted false claims by allegedly failing to maintain a comprehensive care plan "ostensibly required by Medicaid regulation," alongside other relatively minor infractions.
  - –The court explained that the $350 million verdict was inappropriate because the record fatally lacked evidence of materiality and scienter, leaving the verdict based on the theory that "a handful of paperwork defects" and failure to maintain care plans made defendants' claims to Medicare and Medicaid false or fraudulent.
  - –The court noted that Medicare and Medicaid consistently continued to make payments notwithstanding full awareness of "billing and documentation deficiencies."
  - –Finding no evidence that the defendants acted knowingly, the court affirmed the importance of the Supreme Court's *Escobar* decision and its role in enforcing the FCA's materiality standard.
- On May 23, 2018, the United States District Court for the District of South Carolina entered a judgment totaling ~$114 million against three individuals found liable under the FCA of paying kickbacks to physicians in exchange for patient referrals.
  - –The underlying claims initially were brought as part of three lawsuits filed by four whistleblowers, alleging that the kickback scheme caused two laboratories in Virginia and California to bill federal health care programs for medically unnecessary tests.

Environmental
U.S. Update

- Recent analysis* of data from the U.S. Environmental Protection Agency ("EPA") indicates that, under the Trump Administration, civil penalties for pollution fell during the past fiscal year to their lowest average level since 1994.
  - –FY 2018 saw EPA civil fines totaling $72 million, an 85% decrease from the average of more than $500 million per year in the 20 years before President Trump took office.
- Administration officials have asserted that the decline in civil penalties is partially due to their increased focus on working with companies to promote compliance, preventing misconduct instead of punishing it.
- Overall, analysts have found that the monies associated with injunctive relief have fallen dramatically, to the lowest levels since 2003: in FY 2018, companies paid ~$5.6 billion, as compared to the ~$7.8 billion per year average of the prior 20 years.



* Juliet Eilperin and Brady Dennis, *EPA penalties for polluters fell in Trump's first two years, analysis shows,* THE WASHINGTON POST (Jan. 25, 2019)

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

- Although DOJ's Swiss Bank Program wound down at the end of 2016, DOJ's Tax Division announced a number of resolutions in 2018:
  - **Basler Kantonalbank:** a DPA and $60.4 million penalty;
  - **Zürcher Kantonalbank:** a DPA and $98.5 million penalty;
  - **Mirelis Holding S.A:** an NPA and $10.245 million penalty; and
  - **NPB Neue Privat Bank AG:** an NPA and $5 million penalty.
- The Offshore Voluntary Disclosure Program ("OVDP") concluded on September 28.
- On November 20, the Internal Revenue Service ("IRS") announced new voluntary disclosure procedures.
- In December, U.S. prosecutors filed their first charges related to the Panama Papers scandal.

GIBSON DUNN

Focus on Gatekeepers

Continuing Gatekeeper Liability
SEC Update

- The SEC continues to pursue individuals and entities for gatekeeping failures.
  - –70% of the SEC's cases in FY 2018 were brought against individuals.
  - –The SEC brought charges against six accountants for attempting to steal inspection information from the PCAOB, and against three accountants for unprofessional conduct that violated securities laws and auditing standards, such as pre-dating audit paperwork and signing blank audit papers.
  - –The increased focus on cybersecurity issues, including the relatively new frontier of initial coin offerings, has put attorneys and accountants advising on these transactions in the limelight.
- The Supreme Court's February decision in *Digital Realty Trust v. Somers* complicates the whistleblowing calculus. The Court concluded that Dodd-Frank protections for whistleblowers do not apply to external reporting, but only to direct reporting to the SEC.

"Marketing professionals, especially gatekeepers, need to act responsibly and hold themselves to high standards. To be blunt . . . They can do better."

– Jay Clayton, SEC Chairman, Jan. 22, 2018

"Picking and choosing . . . gatekeeper cases [is] extremely important . . . because gatekeepers are the ones who can prevent wrongdoing among any number of actors."

– Lara Shalov Mehraban, Associate Regional Director, SEC New York Regional Office Chairman, Dec. 17, 2018

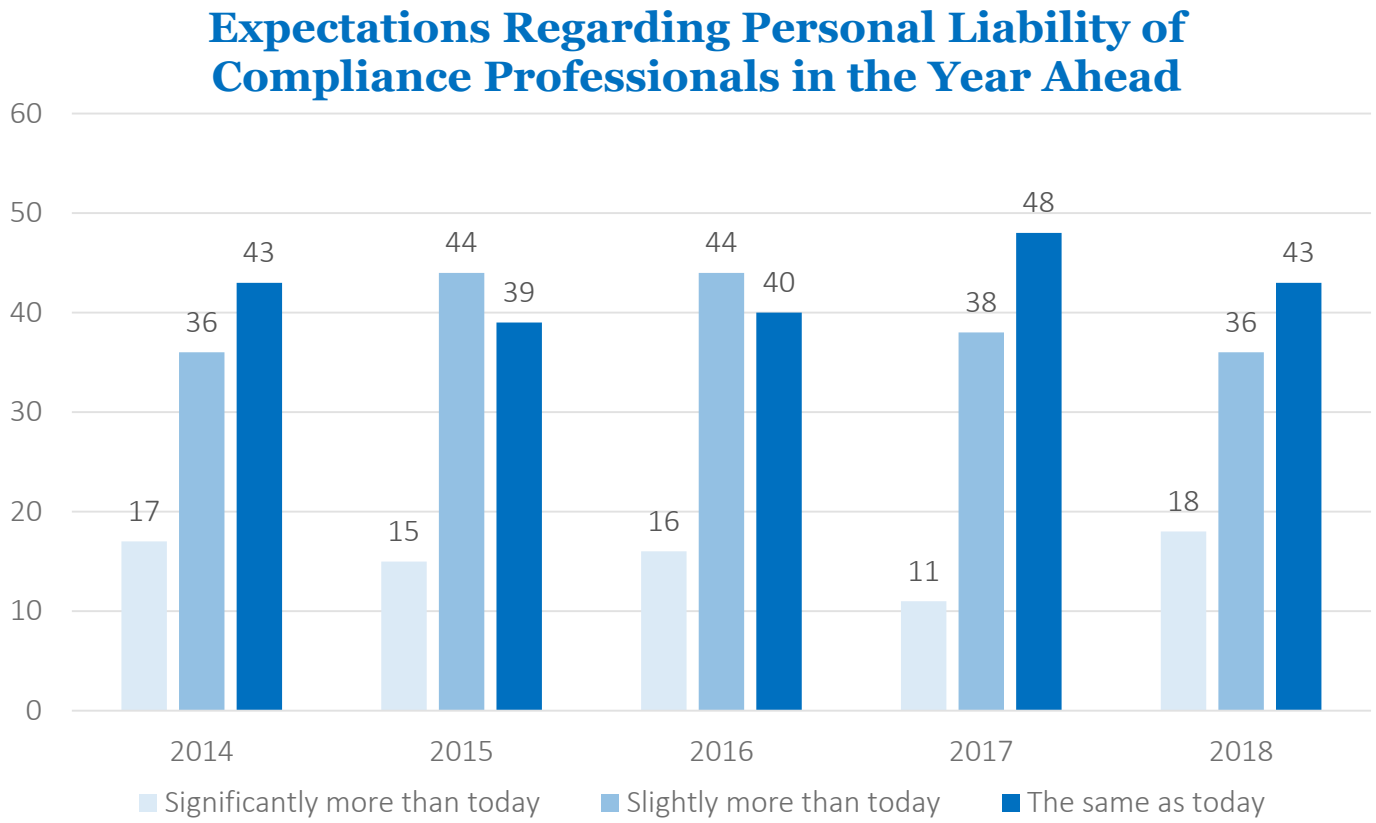
Continuing Gatekeeper Liability
DOJ Update

- DOJ has focused on the investigation and prosecution of compliance professionals for allegedly inappropriate facilitation or participation in misconduct, or otherwise failing to act to professional standards. For example:
  - In its February press release regarding AML/BSA violations by U.S. Bancorp, DOJ specifically attributed responsibility for the violations to the bank's CCO, whom it alleged knowingly presided over an inadequate compliance program and deliberately concealed improper practices from an OCC examiner.
  - In May, the former National Director of Anti-Corruption for Colombia's Office of the Attorney General was extradited from Bogotá on charges related to an alleged bribery scheme, having previously been charged in June 2017 in U.S. federal court with violations including conspiracy to commit money laundering. He allegedly acted through a purported middleman/attorney to corrupt a corruption investigation.
  - In December, DOJ announced the unsealing of an indictment charging four Mossack Fonseca employees—including an attorney and an accountant—with offenses including wire fraud, tax fraud, and money laundering related to the Panama Papers investigation.

Continuing Gatekeeper Liability

Personal Liability of Compliance Professionals

- According to a 2018 survey by Thomson Reuters, more than half of respondent compliance professionals expect their personal liability to increase in the next twelve months:



Thomson Reuters, Cost of Compliance Report 2018

Continuing Gatekeeper Liability

UK/EU Focus on Gatekeeper Liability

- The NCA recently criticized the legal sector in particular for a 10% drop in the number of SARs being submitted by the sector.
- Historically, enforcement figures are low, although professional advisors in the past have faced custodial sentences for failing to report suspicions of money laundering.
- Gatekeepers operating in the "regulated sector" are subject to statutory obligations to report suspected money laundering under the UK Proceeds of Crime Act 2002. This includes lawyers, tax advisors, accountants, and auditors. Money laundering reporting officers also have reporting duties.
- Corporations may also be at risk of prosecution under the Criminal Finance Act 2017 for failing to prevent the facilitation of tax evasion.

On October 31, 2018, UK Minister of State for Security Ben Wallace declared a crackdown on "professional facilitators" of money laundering and sanctions offenses.

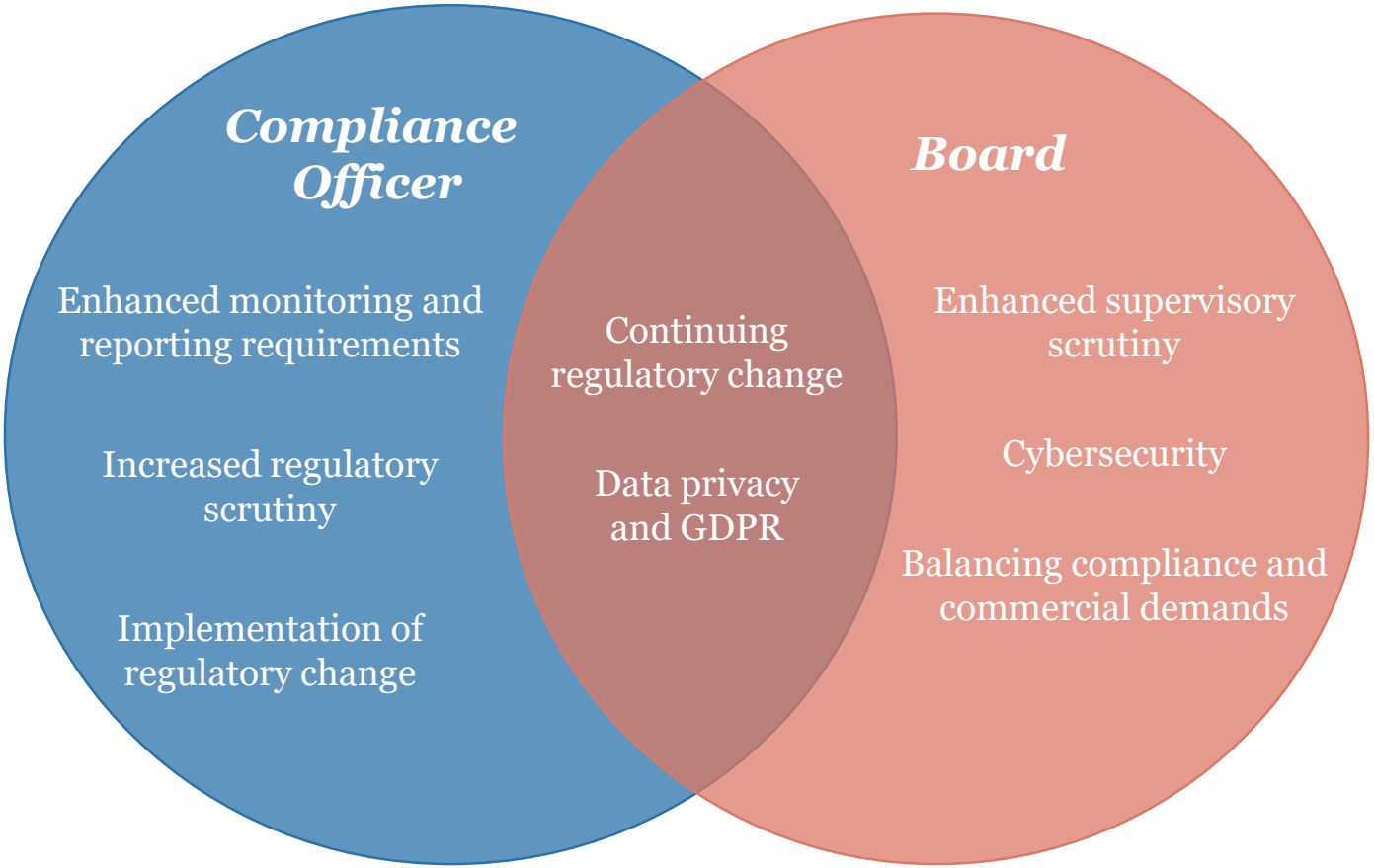
- Separately, lawyers and other professionals, including accountants, auditors, tax advisors, estate agents, and trust or company service providers who fail to report known or suspected sanctions breaches to the Office of Financial Sanctions Implementation ("OFSI") commit a criminal offense.
- Recently, a UK solicitor was sentenced to seven years' imprisonment for money laundering offenses relating to property transactions involving criminal proceeds.

GIBSON DUNN

Building and Overseeing Effective Compliance

Top Compliance Concerns

- In 2018, compliance professionals and boards identified significant areas of concern. Although many of the concerns were consistent with those identified in 2017, compliance officers and boards alike increasingly focused on data privacy and GDPR in 2018.



Thomson Reuters, Cost of Compliance 2018

USSG: Overview of Calculating Corporate Penalties

1. DOJ calculates a "base fine," which corresponds to the greatest of: the "offense level" fine resulting from the specific facts of the crime; the pecuniary gain to the organization; or the pecuniary loss caused by the organization.

2. DOJ calculates the "culpability score," which considers aggravating and mitigating factors, including a pre-existing compliance program, and results in minimum and maximum "multipliers."

3. The base fine is multiplied by the minimum and maximum multipliers to determine the lower and upper bounds of the Sentencing Guidelines range.

4. The Guidelines provide additional factors judges can consider when determining the appropriate fine within (or beyond) the recommended range.

USSG: Role of Compliance in Sentencing

- Factors that can reduce an organization's culpability score, thereby decreasing its Guidelines fine range, include:
  - –The existence of an effective compliance and ethics program; and
  - –Self-reporting, cooperation, or acceptance of responsibility.
- Although companies regularly receive cooperation credit, only a handful have ever received mitigation credit for having an effective compliance program as described in the Guidelines.
- The existence and quality of a company's compliance program appears more likely to factor into DOJ's decision regarding the appropriate resolution vehicle (*e.g.*, NPA or DPA) than to result in a decreased culpability score for purposes of calculating the Guidelines range.

§8B2.1. Effective Compliance and Ethics Program

(a) To have an effective compliance and ethics program, for purposes of subsection (f) of §8C2.5 (Culpability Score) and subsection (b)(1) of §8D1.4 (Recommended Conditions of Probation – Organizations), an organization shall—

(1) exercise due diligence to prevent and detect criminal conduct; and

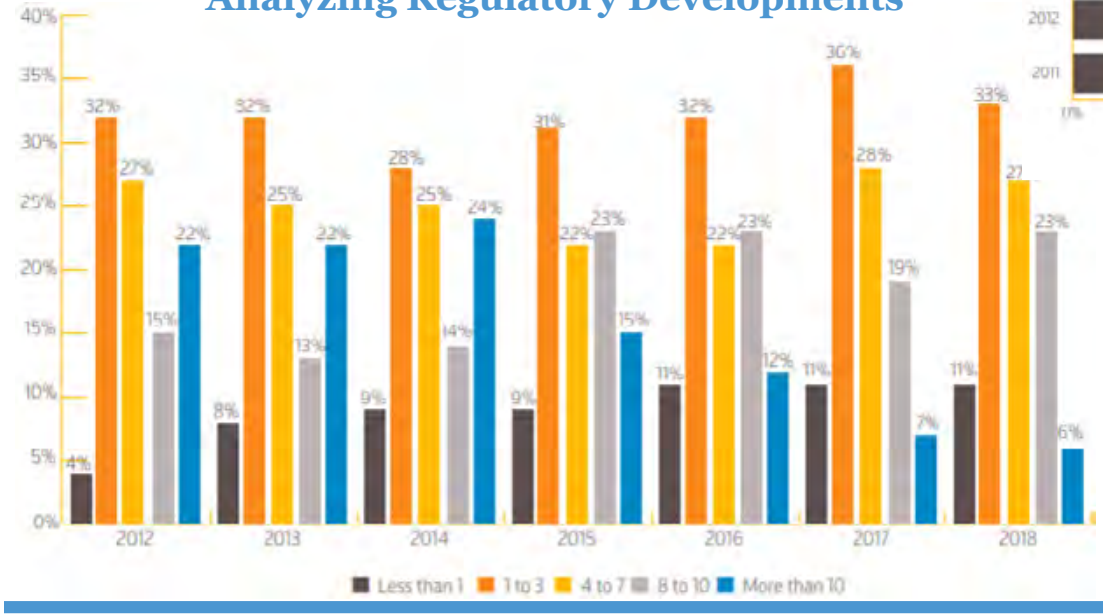
(2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct.

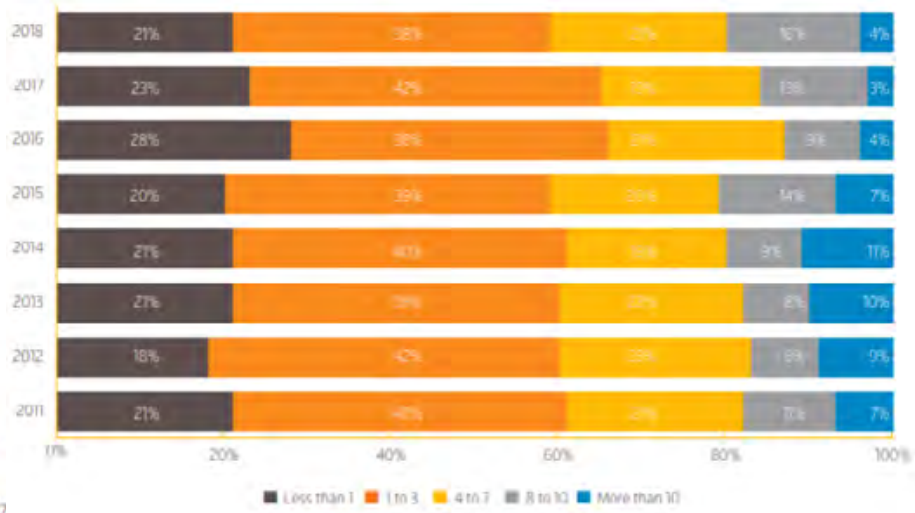
Responding to Regulatory Developments

- As enforcement authorities continue issuing regulations at a staggering pace, compliance professionals report spending a significant amount of time each week tracking, analyzing, and responding to regulatory developments.

Average Hours Spent Tracking and Analyzing Regulatory Developments



Average Hours Spent Amending Policies and Procedures to Reflect Regulatory Changes



Thomson Reuters, Cost of Compliance 2018

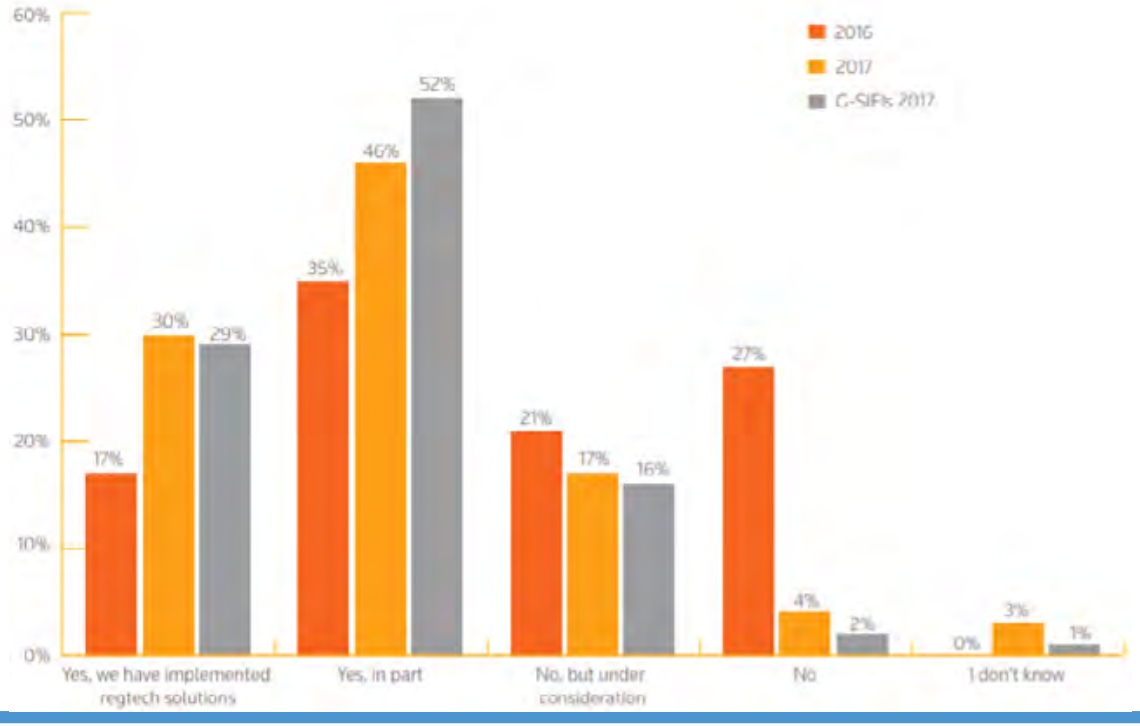
Intersection of Compliance & Technology

- A recent survey shows that many compliance professionals view cybersecurity as a key risk area requiring additional resources to address:
  - **89%** stated that their organization's cybersecurity function does not fully meet their organization's needs.
  - **75%** rated the maturity of their vulnerability identification measures as very low to moderate.
  - **35%** described their data protection policies as ad hoc or non-existent.
  - **12%** stated that their organizations have no breach detection program in place.
- Although companies recognize the significant risks technology poses, they increasingly rely on technological tools to aid with compliance.
  - Companies continue exploring ways to integrate RegTech solutions in their compliance systems. According to one recent survey, **41%** of compliance professionals expect increased compliance involvement in assessing FinTech and RegTech solutions (up from 33% in 2017).

EY 20th Global Information Security Survey, 2017-2018
Thomson Reuters, Fintech, Regtech and the Role of Compliance

Doing More with Less

- Outsourcing certain compliance-related tasks to qualified vendors can improve efficiency and increase flexibility, while allowing companies to focus more on core business activities.
- For compliance activities remaining in-house, companies can utilize dual-hatted employees to expand the compliance function's reach throughout the organization—although companies must provide appropriate training and take steps to avoid conflicts of interest.
- Facing tight budgets and limited resources, compliance departments also are looking to modern, technology-based compliance solutions to help maximize returns.
- Professionals have reported that RegTech already is impacting how they manage compliance.



Thomson Reuters, Fintech, Regtech and the Role of Compliance; Thomson Reuters, Cost of Compliance 2018;

Compliance Trends to Watch in 2019

- ***Eye on regulation:*** Companies are spending more time and money on regulatory compliance—tracking developments, updating policies and procedures, etc.—than ever before.
- ***Data privacy:*** Firms should ensure that their practices are compliant with the markedly evolving landscape of data privacy requirements and regulations, including but not limited to GDPR. Data privacy is a particular challenge for companies with multinational operations.
- ***Cybersecurity:*** The ceaseless onslaught of cyber attacks from both state and non-state actors is one of the most significant challenges that companies will have to face in 2019 and beyond. Regulatory attempts to face this issue bring greater and more exacting compliance obligations for companies big and small.
- ***Gatekeeper liability:*** While regulators have emphasized that they are a resource and a partner for compliance personnel, they also have demonstrated that they will be quick to penalize individuals who actively facilitate or passively allow compliance failures in the organizations where they serve as gatekeepers. The aggressive approach demonstrated by regulators in the past year indicates the importance of diligent attention and timely remediation of potential issues identified.

GIBSON DUNN

Upcoming Gibson Dunn Webcasts & Today's Panelists

Upcoming Gibson Dunn Webcast

February 6, 2019 | 1:00 pm – 2:00 pm EST

The Capital Markets and Private Equity: From Pre-IPO Planning through Public Company Life

Private equity continues to play a prominent role in the life of public and private U.S. companies. This presentation will explain and explore the life cycle of a PE-sponsored public company, from initial acquisition to pre-IPO planning and structuring, governance considerations, and how public companies access the capital markets through private equity. Our team of capital markets and private equity panelists will discuss market trends, legal developments and our recommendations.

Panelists: Andrew Fabens, Andrew Herman, Hillary Holmes, Julia Lapitskaya, Peter Wardle

To Register, **Click Here**

Contact Information

F. Joseph Warin

Partner
Washington, D.C. Office
Tel: +1.202.887.3609
Fax: +1.202.467.0539
FWarin@gibsondunn.com

M. Kendall Day

Partner
Washington, D.C. Office
Tel: +1.202.955.8220
Fax: +1.202.831.6050
KDay@gibsondunn.com

Stuart F. Delery

Partner
Washington, D.C. Office
Tel: +1.202.887.3650
Fax: +1. 202.530.9523
SDelery@gibsondunn.com

Sacha I. Harber-Kelly

Partner
London Office
Tel: +44.20.7071.4205
Fax: +44.20.7070.9205
Sharber-Kelly@gibsondunn.com

Adam M. Smith

Partner
Washington, D.C. Office
Tel: +1 202.887.3547
Fax: +1 202.530.4237
ASmith@gibsondunn.com

Lori Zyskowski

Partner
New York Office
Tel: +1 212.351.2309
Fax: +1 212.351.6309
LZyskowski@gibsondunn.com

Our Offices

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

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

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

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

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

Dubai
Building 5, Level 4
Dubai International Finance Centre
P.O. Box 506654
Dubai, United Arab Emirates
+971 (0)4 318 4600

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, Texas 77002-6117
+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