Hughes Hubbard & Reed

Fall 2018

alert

FCPA & Anti-Bribery

Hughes Hubbard & Reed LLP
A New York Limited Liability Partnership • One Battery Park Plaza
New York, New York 10004-1482 • +1 (212) 837-6000

ANTI-CORRUPTION AND INTERNAL INVESTIGATIONS PRACTICE GROUP

PARTNERS

Kevin T. Abikoff

Derek J.T. Adler

Robert B. Bell

Benjamin S. Britz

Roel C. Campos

Sarah L. Cave

Charles W. Cohen

Ryan Fayhee

Terence Healy

Michael H. Huneke

Edward J.M. Little

Salim Saud Neto*

Matthew R. Nicely

Neil J. Oxford

Laura N. Perkins

Bryan J. Sillaman

Nicolas Swerdloff

George A. Tsougarakis

Marc A. Weinstein

COUNSEL

Tony Andriotis
Olivier Dorgans
Alan G. Kashdan
Daniel J. McLaughlin
Sean M. Reilly
Michael R. Silverman
Nicolas Tollet

ASSOCIATES & INTERNATIONAL SPECIALISTS

Ayoka Akinosi
Ernesto J. Alvarado
Athena Arbes
Rayhan Asat
Ya'ara Z. Barnoon
Tabitha Bartholomew
Elizabeth A. Beitler
Justin Ben-Asher
Gil Ben-Ezra
Arnaldo Bernardi
Megan Buckley
Julia Calafiori*
Ana Carolina Chaves*
Michael A. DeBernardis
Jan Dunin-Wasowicz
Lucie Dzongang
Stephen A. Fowler
Anne Hukkelaas Gaustad
Jaclyn M. Genchi
Chloe Gouache
Jiaxing Hao
Ashley R. Hodges
Maureen A. Howley
Clothilde Humbert
Aylin Ictemel
Adriana Ingenito
Sigrid Jernudd
Jack Kilgard
Robert Kolick
Tamara Kraljic
Clinton T. Lipscomb
Calvin K. Liu
Dorsaf Matri
Jonathan Misk
Megan Mollat
Babaka Mputu
Robby Naoufal
Marie-Agnès Nicolas
Jessica Norrant-Eyme
Miles Orton
Jordan Pate
N. Tien Pham
Antonio Pimentel*
Debbie Placid
Landon D. Reid
Matthew Reynolds
Caroline Rosa*
Mathieu Rossignol
Samuel Salyer
Sergon Sancar
Yoshinori Sasao
Markus A. Stadler
Aleea Stanton
Jennifer Suh
Laura Trumbull
Inès Vally
Shayda Vance
Bernardo Viana*
Laura Vittet-Adamson
Vivian Wang
Adam Weinstein
Scott Yakaitis
Mei Li Zhen
Jonathan Zygielbaum

* Saud Advogados, Rio de Janeiro, Brazil in strategic cooperation with Hughes Hubbard & Reed

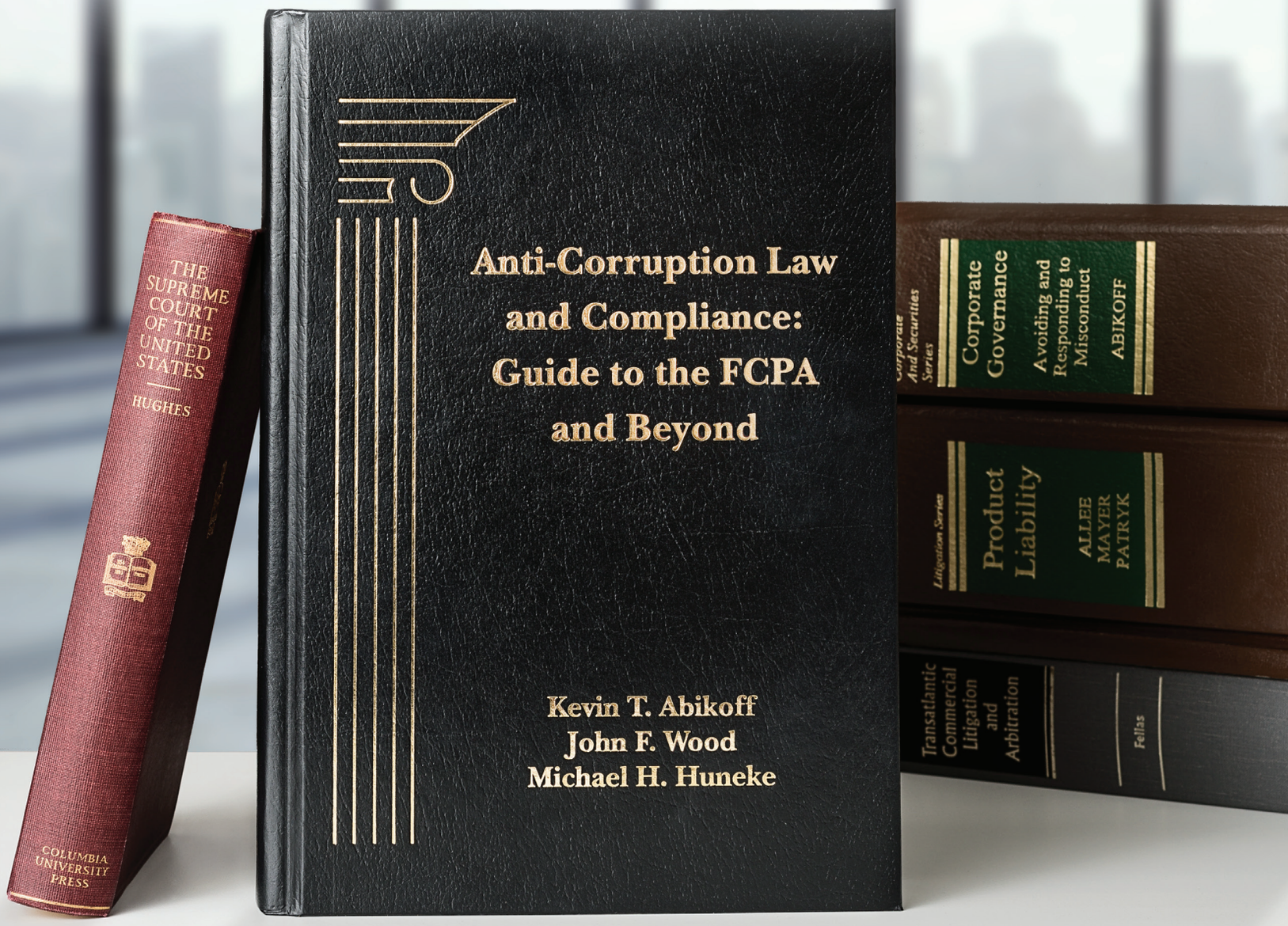
We wrote the book...
and we're still writing them.

Introducing the definitive book on Corporate Governance, the latest in a distinguished line of books by Hughes Hubbard authors dating back to **Charles Evans Hughes** himself.

Hughes Hubbard & Reed

We wrote the book... again.

Introducing the definitive new book on anti-corruption law and compliance, the latest in a distinguished line of books by Hughes Hubbard authors dating back to Charles Evans Hughes himself.



"A powerful and comprehensive resource for anyone dealing with anti-corruption compliance enforcement."
—The FCPA Blog


Kevin T. Abikoff


Michael H. Huneke

Hughes Hubbard & Reed

CONTRIBUTIONS

Editorial Panel:

Kevin T. Abikoff
+1 202 721-4770
kevin.abikoff@hugheshubbard.com

Michael H. Huneke
+1 202 721-4714
michael.huneke@hugheshubbard.com

Laura N. Perkins
+1 202 721-4778
laura.perkins@hugheshubbard.com

Bryan J. Sillaman
+33 (0) 1 44 05 80 03
bryan.sillaman@hugheshubbard.com

Benjamin S. Britz
+1 202 721-4772
benjamin.britz@hugheshubbard.com

Drafting Committee

Michael A. DeBernardis, N. Tien Pham, Jonathan Zygielbaum, Ya'ara Z. Barnoon, Calvin Liu, Clinton T. Lipscomb

Contributors

Ayoka Akinosi, Ernesto Alvarado, Rayhan Asat, Tabitha Bartholomew, Justin Ben-Asher, Gil Ben-Ezra, Megan Buckley, Jan Dunin-Wasowicz, Stephen A. Fowler, Anne Hukkelaas Gaustad, Chloe Gouache, Jiaxing Hao, Clothilde Humbert, Robert Kolick, Leonardo Kozlowski, Tamara Kraljic, Daniel J. McLaughlin, Megan Mollat, Marie-Agnès Nicolas, Jessica Norrant-Eyme, Miles Orton, Jordan Pate, Landon Reid, Mathieu Rossignol, Samuel Salyer, Sergon Sancar, Yoshinori Sasao, Salim Saud Neto, John Schifalaqua, Markus Stadler, Jennifer Suh, Katherine Taylor, Katherine Thomas, Nicolas Tollet, Esther Ullberg, Bernardo Viana, Laura Vittet-Adamson, Vivian Wang, Scott Yakaitis

INTRODUCTION

"I can tell a young person where the mines are,
but he's probably going to step on them anyway."
– Burt Reynolds

The above quote from the late Burt Reynolds could just as easily have been from a dispirited anti-corruption compliance professional in 2018. Despite greater awareness, companies and individuals continue to step on the same proverbial anti-corruption mines. Late 2017 through 2018 saw a considerable number of investigations, prosecutions and settlements based on common and well-established landmarks of violative conduct: the misuse of third party relationships, abuse of gifts, hospitality, and travel, and failure to properly control hiring.

It is clear at this point that just knowing the risks and common mistakes is not sufficient to avoid them. Companies must provide both *guidance* for avoiding the "mines" and *controls* to prevent employees from stepping on them. With this Alert, we hope to help in both respects. Using the past 24 months of enforcement, cases, news, announcements, and policy changes, we will try to help identify the most prevalent and current anti-corruption risks *and* put them in a context so they can be better understood. It is only after understanding the risks that companies can develop guidance and controls to avoid the risks.

This Alert is divided into six chapters. Chapter 1 is devoted to analysis of certain critical enforcement highlights, trends, and lessons from recent settlements, prosecutions, and other related developments. Following that analysis, Chapter 2 is dedicated to the U.S. FCPA. Chapter 2 provides a description of each FCPA-related settlement for 2017 and 2018 organized alphabetically by year. Chapter 2 also includes other relevant FCPA-related developments, including court rulings, guidance, and results from recent FCPA-related civil litigation. Chapter 3 is dedicated to developments in enforcement of the U.K. Bribery Act, including a description of certain recent investigations and enforcement actions of note. Chapter 4 covers enforcement updates in other select countries: Brazil, China, France, and Norway. Chapter 5 provides an update related to the activities of multilateral development banks in the global fight against corruption. Chapter 6 is left for other international developments in the context of anti-corruption enforcement, this year focusing on an update on the status of EU data protection laws and regulations.

For those so inclined, more information is included in our FCPA and Anti-Bribery Compendium, which is freely available on our website (www.hugheshubbard.com) and contains (i) descriptions of all FCPA settlements and criminal matters from 2005 through 2018 (including relevant updates), (ii) a summary of each DOJ Review and Opinion Procedure Release issued from 1980-present, (iii) further details and background information on the U.K. Bribery Act and multilateral development bank enforcement, and (iv) a discussion of various international developments and compliance guidance.

For more information about the matters discussed in this Alert or our Anti-Corruption and Internal Investigations practice generally, please contact us or any member of our Practice Group.

Kevin T. Abikoff
+1 202 721-4770
kevin.abikoff@hugheshubbard.com

Laura N. Perkins
+1 202 721-4778
laura.perkins@hugheshubbard.com

CHAPTER 1: HIGHLIGHTS, TRENDS & LESSONS

I. Recent Highlights

The past year has seen several noteworthy developments in the area of anti-corruption enforcement. Below are Hughes Hubbard's Top 10 highlights from the past twelve months. This year, in the tradition of *Spinal Tap*, we have gone one louder—to 11.

1. Corporate Enforcement Policy

In November 2017, Deputy Attorney General Rod Rosenstein announced that the DOJ had adopted a Corporate Enforcement Policy to encourage voluntary reporting of FPCA violations and set standards for cooperation and remediation credit. The Corporate Enforcement Policy formalized the FCPA Pilot Program from April 2016 with tweaks that further incentivize companies to voluntarily report FCPA violations. Most prominently, the Corporate Enforcement Policy created a rebuttable presumption that the DOJ will decline to prosecute a company that voluntarily discloses a violation, cooperates with the DOJ investigation, agrees to disgorge illicit profits, and takes appropriate remedial measures. The Corporate Enforcement Policy, with its various requirements and caveats (such as requiring companies to prohibit the use of self-deleting messaging apps), has the ability to impact FCPA investigations as much as any other development of the past five years. The benefits for eligible companies are real and material. But to avail themselves of those benefits (whether a company decides to voluntarily disclose the misconduct or not), companies must act quickly and strategically in responding to evidence of allegations of misconduct. If nothing else, the Corporate Enforcement Policy adds pressure on companies to establish a clear understanding of the facts and circumstances of potential misconduct as soon as possible in order to make an informed and reasoned disclosure decision.

2. *U.S. v. Hoskins*

On August 24, 2018, the U.S. Court of Appeals for the Second Circuit affirmed a district court holding that prosecutors could not properly charge Lawrence Hoskins, a British national and former Alstom executive, with conspiracy to violate the FCPA. Hoskins was allegedly part of a scheme to bribe Indonesian officials in order to obtain a $118 million contract from the Indonesian government. But, while he communicated by phone and by email with his alleged co-conspirators in the U.S., Hoskins remained outside of the U.S. during the entirety of the alleged conspiracy. The Second Circuit found that foreign nationals may only violate the FCPA with action outside of the United States if they are agents, employees, officers, directors, or shareholders of an American issuer or domestic concern. As a result, the Second Circuit affirmed the dismissal of the conspiracy charge to the extent the charge was grounded on a theory that Hoskins acted "together with a domestic concern" or "while in the territory of the United States" but explicitly held open the government's argument that Hoskins was acting as an agent of Alstom's U.S. subsidiary. While the holding of *Hoskins* could be narrowly read to apply solely to conspiracy charges, the court's detailed analysis of the FCPA's legislative history and its

applicability to foreign nationals outside of the U.S. promises a wider area of effect. Its application (or rejection) by other courts in the next year may shape the nature of FCPA charges going forward.

3. "Piling On" Policy

On May 9, 2018, Deputy Attorney General Rod Rosenstein announced a new DOJ policy, to be incorporated into the U.S. Attorneys' Manual, discouraging the practice of "piling on"—imposing excessive or redundant penalties—in corporate enforcement actions. The policy instructs DOJ attorneys to coordinate with attorneys in other DOJ components that are investigating the same corporate misconduct, and with other domestic and foreign enforcement agencies (when possible), to achieve equitable results. This policy represents a positive development for companies subject to multiple authorities, as it tightens the focus of U.S. FCPA enforcement efforts on the anti-corruption aims of the statute and recognizes the dangers and costs to international business of "piling on," by encouraging DOJ attorneys to work with enforcement and regulatory agencies to avoid repeated or excessive punishment for the same misconduct.

4. Petrobras

In September 2018, Petrobras entered into a $1.78 billion global settlement with Brazilian and U.S. authorities related to bribes paid to senior Brazilian officials. Not only is the Petrobras settlement easily the largest of the last 12 months, it represents a capstone to the highly publicized (and highly successful) Operation Car Wash. What started as a small-scale money laundering investigation ballooned into a massive, unprecedented corruption investigation that reached not just into state-owned Petrobras, but to the highest levels of the Brazilian government. Moreover, the fact that Petrobras is state-owned is additional proof that U.S. and other regulators will not hesitate to prosecute corruption and other misconduct, regardless of the ownership of the entity.

5. SEC v. Cohen

On July 12, 2018, the district court in the Eastern District of New York ruled that the SEC's highly publicized claims against Och-Ziff employees Michael Cohen and Vanja Baros related to Och-Ziff's corrupt activities were time-barred. In particular, the court found that the SEC's claims for injunctive relief were subject to the standard five-year limitation period from when the violation occurred, a break from courts in other circuits which have held that injunctive relief (in contrast to other types of penalties and relief) is not subject to this limitation. To the extent other courts agree with the *Cohen* court's analysis, the decision would serve to greatly limit the SEC's ability to bring FCPA claims for conduct more than five years old.

6. Panasonic's Resolutions with DOJ and SEC

In April 2018, Panasonic Corporation and its U.S.-based subsidiary, Panasonic Avionics Corporation ("PAC"), agreed to pay more than $280 million in combined fines, fees, and

disgorgement to resolve FCPA charges with the DOJ and SEC. The settlements with the DOJ and SEC were noteworthy in a number of respects (aside from the approximately $280 million price tag). Among other things, the settlements highlight the dangers and risks associated with hiring *former* public officials as representatives or employees. According to charging documents, while negotiating an amendment to a supply agreement with a state-owned airline, PAC had discussions with an official of the airline about a well-paying position with PAC. After the negotiations concluded, the official resigned from his position with the airline and took a position as a consultant with PAC. While the risks of hiring current government officials are well understood, Panasonic's resolution is a prime example of why companies must be cautious when engaging former public officials as well, particularly when the official was previously in a position to influence relevant business.

7. Credit Suisse

In May and July 2018, Credit Suisse agreed to pay approximately $75 million to resolve investigations by the DOJ and SEC into Credit Suisse's illicit referral hiring program in the Asia-Pacific region. After a couple of quiet years, the "Sons and Daughters" program historically utilized by many banks and other companies in China and other parts of Asia was again the focus of a major FCPA resolution. Credit Suisse's settlements with the DOJ and SEC serve as a stark reminder of the risks associated with hiring relatives of foreign government officials. They also serve as a reminder that even appropriately designed policies and procedures offer little protection to companies absent effective implementation and oversight. Credit Suisse maintained policies that explicitly prohibited the conduct that led to the resolution. As is obvious from the resolution, such well-intentioned policies and procedures are not enough if not accompanied by effective implementation and monitoring.

8. GDPR

After several years of anticipation, the European Union General Data Protection Regulation ("GDPR") entered into force in all E.U. Member States. As companies scramble to ensure compliance with the GDPR in connection with everyday business, lawyers and compliance personnel also have to deal with its requirements in conducting internal investigations. In particular, companies and counsel must carefully consider the need for employee consent prior to collecting and reviewing employee data and must ensure that all requirements are followed before any data can be transferred outside of the E.U. While the full impact remains to be seen, it is clear that careful planning and documentation are critical in connection with internal investigations involving employees or activity in the E.U.

9. Société Générale

In June 2018, Société Générale and its wholly-owned subsidiary, SGA Société Générale Acceptance N.V. ("SGA"), agreed to pay a total of $585 million to U.S. and French authorities in order to resolve a coordinated investigation into a multi-year scheme to

bribe Libyan officials. The resolution involved the first-ever joint resolution between the United States and France on a corruption case. Société Générale's settlement with French authorities demonstrates that France will not be afraid to utilize the new tools authorized or enhanced by Sapin II, such as criminal corporate settlements and monitoring by the new French anti-corruption agency.

10. The Siemens Prosecution That Never Ends

In 2008, Siemens set the anti-corruption world on fire with what was then the largest ever corruption resolution, over $1.6 billion to U.S. and German authorities, dwarfing previous settlements to that point. Ten years later, individuals involved in Siemens' various schemes are still being prosecuted. In 2018, Eberhard Reicher was arrested and pleaded guilty for his role in Siemens' corrupt practices in Argentina. Reicher and seven co-conspirators were indicted in 2011 but have been living abroad and avoiding prosecution since that time. Of the eight total co-conspirators, six remain at large. The continuing prosecutions of participants in the Siemens scheme serves as a timely reminder of the groundbreaking nature of that resolution, both in size and scope, and how far the world has come in terms of anti-corruption enforcement since that time.

11. ENRC

In a decision that has been widely applauded by the legal community, the English Court of Appeal overturned much of the High Court's decision that materials prepared by counsel in connection with internal investigations, including interview notes, are not entitled to protection of the attorney-client privilege. On May 8, 2017, Justice Andrews of the High Court of Justice, Queen's Bench Division, handed down a decision in *Serious Fraud Office v. Eurasian Natural Resources Corporation* presenting a restrictive interpretation of both forms of legal privilege in the U.K., litigation privilege and legal advice privilege, as applied to documents created during an internal investigation. With regards to litigation privilege, the Court of Appeal held that anticipating a criminal investigation fulfills the requirement that adversarial litigation is reasonably in contemplation. The Court of Appeal also found that the evidence demonstrated that the documents at issue were created for the dominant purpose of resisting the contemplated criminal proceedings, and that it was of no issue that ENRC considered sharing materials from its investigation with the SFO as part of its negotiation strategy. The decision by the Court of Appeal eased significant concern of companies and white collar practitioners in the U.K. and beyond about the protection afforded to materials prepared by counsel in connection with an internal investigation.

II. Trends & Lessons

The combination of resolved actions, ongoing criminal and regulatory investigations, guidance issued by regulatory authorities, and other developments discussed below underscore a number of important themes of which companies should be aware in conducting their operations, designing and implementing their compliance programs, considering whether to enter into potential transactions or to

affiliate with an international agent, intermediary, or joint venture partner, and dealing with government agencies. These themes take the form of both enforcement trends and practice lessons.

A. Trends

- *International Coordination:* The DOJ and SEC continue to rely upon and provide assistance to a growing number of non-U.S. enforcement agencies in complex bribery investigations. The DOJ credited authorities from the following countries for assistance in its FCPA prosecutions in 2018 and 2017: Austria, Belgium, Brazil, British Virgin Islands, Cyprus, Dominican Republic, France, Germany, Guinea, Ireland, Isle of Man, Israel, Latvia, Luxembourg, Mexico, the Netherlands, Norway, Singapore, South Africa, Switzerland, and the United Kingdom.

  Moreover, since the beginning of 2017, four FCPA resolutions have been coordinated with parallel resolutions by foreign governments: (i) Telia Company AB (Netherlands), (ii) Keppel Offshore & Marine Ltd. (Singapore, Brazil), (iii) Société Générale S.A. and the related resolution with Legg Mason (France), and (iv) Petroleo Brasileiro S.A.—Petrobras (Brazil). All four rank among the top ten largest FCPA resolutions, with Petrobras ($1.78 billion) and Telia ($965 million) occupying the top two spots. This continued a trend from 2016, which saw five cases resolved with parallel resolutions, including VimpelCom (Netherlands), the fourth largest FCPA settlement to date. According to the enforcement agencies themselves, the coordination of penalties was made possible by the cooperation of the companies involved. The importance of the coordination in these resolutions should not be overlooked. In all four cases since 2017, the total criminal penalty was calculated according to the U.S. Sentencing Guidelines, with the United States and foreign authorities dividing the total penalty amount among themselves. Careful coordination of resolutions in this manner may help to ensure that a company is not penalized twice for the same conduct. Nevertheless, these global resolutions have come at a significant cost. In total these four companies agreed to pay more than *$3.5 billion* in fines, disgorgement, and prejudgment interest.

- *Other Third Party Risks:* For years, regulators, practitioners, and compliance professionals have been warning of the corruption risks associated with sales agents and consultants. The use of these third parties was, and continues to be, a favorite source for corrupt actors to disguise their illicit actions. However, enforcement over the past two years demonstrates the real and growing risks associated with other types of third parties, such as distributors, dealers, and subcontractors. For example, the SEC's cease and desist order against UTC details the failure of UTC subsidiaries to perform due diligence on subcontractors and obtain adequate proof of service. The SEC also alleged that UTC's subsidiary used discounts to distributors to create slush funds through which bribes could be paid. The SEC's $25 million resolution with Sanofi was similarly based, in part, on Sanofi's use of distributors to allegedly disguise bribe payments. A similar scheme was allegedly used by Orthofix to funnel bribe payments to doctors at state-owned hospitals, resulting in a settlement with the SEC in 2017.

- *Successful Challenges to Enforcement:* Over 35 individual prosecutions and civil actions related to the FCPA have been initiated since 2017. This level of enforcement is consistent with statements from the DOJ and SEC that individuals would be held accountable for their

improper actions. However, because individuals are less likely than corporations to plead guilty or even accept the jurisdiction of U.S. authorities, the increase in individual prosecutions appears to have led to an increase in litigation. As a result, case law is now being produced by American courts regarding the FCPA that may have potentially lasting consequences on enforcement actions going forward.

Notably, in July 2018, Judge Nicholas Garaufis in the Eastern District of New York dismissed the SEC's charges against Michael L. Cohen, a former partner at Och-Ziff and member of the firm's management committee, and Vanja Baros, a former Och-Ziff analyst who was a member of Och-Ziff's African Special Investment Team, as time-barred. Applying the Supreme Court's holding in Kokesh, the court found that the SEC's requested relief of civil penalties, disgorgement, and an injunction against future securities offenses were penal in nature and thus subject to the five-year statute of limitations in 28 U.S.C. § 2462. In August 2018, the U.S. Court of Appeals for the Second Circuit held that the DOJ could not bring conspiracy charges against Lawrence Hoskins, a former Alstom executive, because the FCPA's language evinced an intent to exclude non-resident foreign nationals like Hoskins (a British national) from the statute's provisions unless they were an employee or agent of an issuer or domestic concern or they took action while in the United States. It is not yet clear whether this position will be adopted by other courts, but defendants, including Ukrainian billionaire Dmitry Firtash, have already sought to dismiss charges based on the Second Circuit's decision.

Both the *Hoskins* and *Cohen* decisions have the potential to impact FCPA prosecutions against individuals and corporations, and, in the end, both may serve to limit U.S. authorities' ability to reach certain defendants, a bittersweet outcome to the SEC's and DOJ's efforts to increase enforcement against individuals.

- *Size of Penalties:* The waning months of the Obama administration saw a number of massive corporate FCPA settlements. At the time, it wasn't clear if these settlements were an aberration or a sign of things to come. The size of FCPA settlements since then has varied. 2017 saw only one corporate resolution with similar financial penalties. As part of its global resolution with the DOJ, SEC and Public Prosecution Service of the Netherlands, Telia Company AB agreed to pay a total of $965 million to resolve bribery allegations (*see* p. 67). In 2018, however, there have already been 3 settlements in excess of $200 million. Société Générale agreed to pay more than $585 million as part of a global resolution with U.S. and French authorities. Panasonic and its subsidiary agreed to pay a combined $280 million to resolve SEC and DOJ investigation. Finally, in September 2018, Petrobras agreed to pay $1.78 billion to U.S. and Brazilian regulators to resolve the long-running corruption investigation into the Brazilian state energy company (*see* p. 39).

- *U.S. Law Enforcement Cooperation*: In addition to cooperation with foreign agencies, the DOJ and SEC credited a wide variety of domestic agencies and divisions for their assistance in various of its investigations in 2017 and 2018: (i) FBI, (ii) IRS Criminal Investigation, (iii) ICE Homeland Security Investigations, (iv) U.S. Postal Inspection Services, (v) the Federal Reserve Bank of New York, (vi) DOE OIG, and (vii) the CFTC. It is clear that U.S.

prosecutors have vast and varied resources available to investigate foreign bribery allegations.

- *Pharma Remains in the Cross-Hairs*: – Last year in this space we noted the number of recent FCPA cases against pharmaceutical, health science, and medical device companies. The trend held true through 2018. Both Sanofi (*see* p. 42) and Stryker (*see* p. 45) settled FCPA cases in 2018. Moreover, the Stryker and Sanofi cases are classic examples of what has become perhaps the biggest anti-corruption risk for healthcare companies operating abroad: the use of distributors and sub-distributors.

- *Prosecution of Foreign Government Officials:* Recent actions have made clear that U.S. prosecutors will not hesitate to prosecute the foreign government officials that are on the receiving end of bribes. Although such officials are not covered under the FCPA (which prohibits only active bribery), U.S. prosecutors have successfully used money laundering laws to prosecute several foreign government officials over the past 24 months. *See* Heon Cheol Chi (p. 53), Mahmoud Thiam (p. 66), Koolman and Parker (p. 33), and PDVSA Procurement (p. 36).

- *Expansive Assertion of Anti-Corruption Jurisdiction:* For years, U.S. regulators have taken an expansive jurisdictional view as to the applicability of the FCPA. "Issuers" are subject to the accounting provisions of the FCPA regardless of what action, if any, is taken in the United States. For example, in 2018, Sanofi, the French pharamceutical company whose shares have traded on the New York Stock Exchange since 2002, settled books and records and internal controls violations with the SEC for conduct that took place entirely in the Middle East and Kazakhstan (*see* p.42). However, for foreign nationals and corporations (even foreign issuers), territorial jurisdiction must exist for violations of the anti-bribery provisions. The DOJ's arguments for territorial jurisdiction have previously been attenuated, including for example, seeking to create territorial jurisdiction solely on the basis of emails sent through the United States or the use of a U.S. bank account. However, as shown by the Second Circuit's decision in *Hoskins*, it is far from clear whether such jurisdictional arguments would be upheld if challenged in court.

- *Focus on High-Risk Jurisdictions*: Not surprisingly, the conduct that led to the various enforcement actions over the past two years was largely concentrated in countries with a known history of pervasive corruption. Among the most prevalent, China featured in seven enforcement actions in 2017 and 2018 and Brazil in four enforcement actions.

- *Growing Interest in DPAs*: Deferred Prosecution Agreements are an effective and commonly-used tool in anti-corruption enforcement. DPAs give companies the option to resolve an impending criminal action early, potentially without the cost and collateral consequences that correspond with a criminal action. While DPAs have been in use in the United States for quite some time, and are regularly-used in FCPA enforcement, interest in DPAs as an effective tool in anti-corruption enforcement among foreign regulators is growing as well. The U.K. and France have each recently adopted, and used, DPAs or DPA-equivalents in anti-corruption enforcement. Following its groundbreaking resolution with Keppel Offshore & Marine, Singapore has passed legislation introducing DPAs into its criminal procedure code.

In 2018, Canada also proposed legislation to allow for the use of DPAs. As more and more countries gain experience in investigating and prosecuting corruption, it would be little surprise to see the use of DPA-like mechanisms to continue to spread.

- *Emphasis on Timely Remediation:* The DOJ and SEC have long signaled that extensive cooperation with their investigations and full remediation may result in less severe penalties. Past enforcement has demonstrated that the DOJ and SEC expect cooperation to be timely and will offer less credit to companies who delay in cooperating. Enforcement in 2018 demonstrated that the DOJ and SEC also consider timely remediation to be of paramount importance. In its April 2018 DPA with Panasonic, the DOJ afforded Panasonic "only" 20% off of the low end of the U.S. Sentencing Guideline range rather than the 25% for which Panasonic was otherwise eligible. Given that the DOJ credited Panasonic's cooperation and remedial measures, it is reasonable to assume that Panasonic was docked 5% as a result of its "delayed" remedial measures.

- *Credit for Management Changes:* Regulators may use enforcement actions as carrots or sticks, either to force changes in management where the regulators believe management is insufficiently attuned to corruption concerns, or to reward companies that change management in response to findings of misconduct. This view has been borne out in settlement language. For example, in Keppel Offshore & Marine Ltd.'s ("KOM") 2018 resolution with the DOJ, the DOJ afforded KOM the full 25% off of the bottom of the U.S. Sentencing Guidelines range, highlighting that KOM disciplined or terminated culpable employees and imposed $8.9 million in disciplinary sanctions on current and former employees. Meanwhile, failure to appropriately discipline all individuals involved can result in more severe penalties. For example, despite fully cooperating with the DOJ and SEC investigations, Credit Suisse received a 15% discount off of the bottom of the Sentencing Guidelines penalty range, rather than the full 25% for which it was otherwise eligible. The DOJ noted that while Credit Suisse fully cooperated with the investigation and conducted a number of remedial measures, it failed to sufficiently discipline employees involved in the misconduct.

B. Lessons from Recent Enforcement Activity

- *Adequately and Appropriately Investigate and Respond to Allegations*: Enforcement agencies expect companies to adequately and appropriately investigate allegations or evidence of misconduct. The Corporate Enforcement Policy announced in 2017 places extra pressure on companies to respond fully and as quickly as possible. In order to take advantage of the benefits of the Corporate Enforcement Policy, companies must understand the nature of potential misconduct as quickly as possible and, in any event, pror to the news reaching the DOJ.

  Identification by internal or external auditors of red flags or suspicious conduct has also been used by enforcement agencies as evidence of companies' knowledge of and failure to stop improper practices. For instance, in its 2018 settlement with Panasonic Aviation Corporation (*see* p. 34), the DOJ noted that as early as September 2010 Panasonic's Internal Audit Department issued a report identifying a number of compliance risks associated with

Panasonic's use of one service provider to engage other third party consultants and stated clearly that the consultant payments should be "carefully reviewed in light of FCPA regulation [sic] due to lack of clarity in deliverables." However, nothing was done and, by December 2010, an abbreviated version of the report began to circulate with that critical conclusion removed.

- *Need for Appropriate Due Diligence and Monitoring of Business Partners*: The vital importance of risk-based due diligence of third parties is one of the most important lessons to guide the development and implementation of an effective corporate compliance program. The DOJ's Compliance Guidance released in February 2017 explicitly states that the DOJ will look to whether the company has in place risk-based controls for engaging and monitoring third-parties. This focus on the importance of effective risk-based due diligence has also been embraced by the international community. OECD guidance on internal controls, ethics, and compliance programs counsels towards the adoption of a risk-based approach to due diligence. The World Bank Integrity Compliance Guidelines and African Development Bank Integrity Compliance Guidelines also require that companies have in place a process for risk-based due diligence on all third parties.

  The importance of due diligence on third parties has also been borne out in recent enforcement actions. Eleven of the 13 U.S. corporate settlements and prosecutions in 2017 and 2018 involved third-party agents or intermediaries. In almost every one of those cases, the DOJ or SEC criticized the companies for failing to conduct appropriate due diligence on their third-party agents or intermediaries, or for ignoring red flags that suggested that there was a high probability that the payments to such entities would be passed on to government officials. For example, in the Elbit Imaging order (*see* p. 29), the SEC criticized the company for paying $14 million to two offshore entities to help obtain an investment invitation and development approvals from Romanian officials without conducting any due diligence on the entities or demanding any documentation demonstrating that services were actually provided.

  - *Determine Identities of Beneficial Owners:* Shell companies and other similar entities can easily be used to conceal the identities and locations of their beneficial owners, and thus the true source or destination of funds. Any due diligence procedure must seek to learn the identities of all beneficial owners and actual control persons of shell companies, holding companies, and trusts that maintain an ownership interest in an agent or third party. The 2017 case against SBM and its American subsidiary (*see* p. 61) illustrates the risks of failing to implement a process to identify beneficial owners of third-party companies. SBM entered into various arrangements with a Brazilian consultant to transmit "commission" payments to the consultant's Brazilian bank accounts and to accounts maintained in Switzerland by the consultant's British Virgin Islands-based shell companies. Funds transferred to the shell companies' bank accounts were used to make bribe payments to officials at Petrobras, often to those officials' own Swiss bank accounts.

  - *Examine Carefully the Qualifications of Agents, Distributors, and other Third Parties:* Companies must understand the background and qualifications of agents and intermediaries. The SEC criticized UTC and its subsidiaries (*see* p. 49) for example, for

engaging an agent that did not have any experience in the relevant industry, and who was, until engaged by UTC to sell airplane engines and associated services, primarily focused on the toll-road industry. Third parties that are insufficiently qualified or that have no discernable operations (i.e., "brass plate" or "mailbox" companies) should be avoided. Although distributors have traditionally been viewed as presenting less corruption risk than sales agents, the 2018 enforcement actions against Sanofi and UTC demonstrate that the qualifications, activities and payment structures associated with distributors should be evaluated as well.

- *Examine Carefully Tasks to be Performed by Third Parties:* Companies must examine the specific tasks that a third party will perform, and the justification for retaining the third party to perform those tasks. Companies should also validate the tasks allegedly being provided by the third party. In 2017 and 2018, enforcement actions against Colin Steven, Elbit Imaging Ltd., Kinross Gold, Panasonic Avionics Corporation, Telia, and PDVSA suppliers Rincon & Shiera all involved third parties paid through agreements for nonexistent services.

- *Ensure that Compensation is Commensurate with Services*: Once validating the services provided by the third party, companies must ensure that the compensation is commensurate with those services. Even with no other risk factors, excessive compensation can be a significant red flag, particularly in high risk jurisdictions.

- *Beware of Local Content Requirements*: Local content requirements have long caused difficulties for companies operating in high-risk jurisdictions. The lack of local expertise can make it difficult to meet local content requirements through hiring local companies and individuals for legitimate services. These problems are exacerbated by corrupt local officials willing to game the system by setting up local companies and suggesting (or requiring) that such companies be engaged to meet local content requirements. Halliburton's 2017 settlement with the SEC (*see* p. 51) demonstrates these difficulties and highlights the importance of maintaining strict internal controls in the procurement context.

- *Compliance Programs and Internal Controls Must be Effective at Preventing Misconduct:* Year after year, enforcement actions illustrate that simply maintaining a compliance program is not enough. Compliance programs and internal controls must be adequate and effective at preventing and detecting misconduct. Recent enforcement actions have reflected a willingness by the SEC to pursue FCPA claims even when companies have established compliance programs at the time of the misconduct and the employees involved intentionally evaded the controls in place. Halliburton, for example, established tight rules and regulations regarding retaining third party agents and other vendors. Nevertheless, because an employee in Angola was able to circumvent these controls, the SEC took the position that such controls were inadequate. More recently, in 2018 the SEC found that Panasonic had failed to maintain adequate internal controls because, among other things, the company's employees were able to evade third-party due diligence requirements. The SEC noted that Panasonic's due diligence procedures were ineffective because employees were able to engage sales agents as subagents of a third party that had successfully completed the due diligence process. According to the SEC, PAC employees were able to direct payments to

13 uncertified third parties through one agent that had successfully completed the due diligence process. On the other hand, in 2012 both the DOJ and SEC declined to charge Morgan Stanley despite misconduct by an employee, discussing in detail how the company maintained a robust and largely effective compliance program.

These enforcement actions underscore the importance to companies of continuously testing and reviewing their compliance programs to ensure that they are adequately designed to prevent misconduct.

- *Conduct Effective M&A Due Diligence*: Pre-acquisition or post-acquisition anti-corruption due diligence is now a regular part of most corporate acquisitions. The pressure to ensure that such due diligence is effective in identifying potential misconduct is as high as ever. In 2017, Mondelēz settled FCPA charges with the SEC related to the activity of Cadbury, which Mondelēz acquired in 2010 (*see* p. 57). Although the SEC acknowledged that Mondelēz conducted substantial post-acquisition due diligence, such due diligence failed to identify the misconduct of Cadbury. As a result, Cadbury's relationship with a particularly problematic agent continued for eight months and Mondelēz was held to be responsible for the violations of Cadbury.

- *Structure and Staff Compliance Functions Appropriately*: Government regulators have emphasized the need for companies to take measures to ensure that their compliance obligations are taken seriously at the highest level of management and that the compliance function is appropriately structured, staffed, and funded. Government authorities, for example, criticized VimpelCom's lack of adequate compliance structures and personnel. At the time of its purchase of the two subsidiaries through which payments were made, VimpelCom had no Chief Compliance Officer, and the individual later hired for this role was considered by the authorities to be underqualified and inadequately resourced.

- *Apply Close Scrutiny to High Risk Subsidiaries or Units*: The April 2018 SEC enforcement action against Dun & Bradstreet, for example, was based on the actions of two Dun & Bradstreet subsidiaries in China. One of Dun & Bradstreet's subsidiaries formed a joint venture with a local firm, but even after learning that this local firm had used its government connections to source non-public and restricted information from government agencies, Dun & Bradstreet failed to adopt controls that could prevent such behavior. Instead, Dun & Bradstreet merely provided a short FCPA training to executives of the joint venture partner and required the joint venture to source such information through third parties. Dun & Bradstreet also acquired another company in China that purchased data from third-party vendors. Although Dun & Bradstreet uncovered significant red flags during its pre-acquisition due diligence on this local entity, the Company failed to follow up on these red flags after the acquisition. Dun & Bradstreet's settlement demonstrates the need for companies to closely scrutinize the activities of high-risk subsidiaries, and to implement compliance controls that adequately address the risks presented by such operations.

CHAPTER 2: FCPA

I. FCPA Elements and Penalties

The FCPA has two fundamental components: (1) the Anti-Bribery Provisions in Section 30A of the Securities Exchange Act of 1934 ("Exchange Act")[1] and in Title 15, United States Code,[2] and (2) the Books and Records and Internal Accounting Control Provisions in Sections 13(b)(2)(A)[3] and 13(b)(2)(B)[4] of the Exchange Act, respectively (collectively, the "Accounting Provisions"). The DOJ has exclusive jurisdiction to prosecute criminal violations of the FCPA, while the DOJ and the SEC share jurisdiction over civil enforcement actions.

A. Anti-Bribery Provisions

The FCPA's Anti-Bribery Provisions prohibit: (i) an act in furtherance of (ii) a payment, offer or promise of, (iii) anything of value, (iv) to a foreign official,[5] or any other person while knowing that such person will provide all or part of the thing of value to a foreign official, (v) with corrupt intent, (vi) for the purpose of either (a) influencing an official act or decision, (b) inducing a person to do or omit an act in violation of his official duty, (c) inducing a foreign official to use his influence with a foreign government to affect or influence any government decision or action, or (d) securing an improper advantage, (vii) to assist in obtaining or retaining business.[6]

The term "foreign official" is broadly defined to mean any officer or employee of a foreign government, agency or instrumentality thereof, or of a public international organization, or any person acting in an official capacity on behalf of such government, department, agency, or instrumentality, or public international organization.[7] The term foreign official has been construed by federal prosecutors to include employees, even relatively low-level employees, of state-owned institutions.

Under the FCPA, "a person's state of mind is 'knowing' with respect to conduct, a circumstance, or result" if he or she has actual knowledge of the conduct, circumstance or result or "a firm belief that such circumstance exists or that such result is substantially certain to occur."[8] In addition, knowledge of a circumstance can be found when there is a "high probability" of the existence of such circumstance.[9] According to the legislative history,

> [T]he Conferees agreed that "simple negligence" or "mere foolishness" should not be the basis for liability. However, the Conferees also agreed that the so called "head-in-the-sand" problem—variously described in the pertinent authorities as "conscious disregard," "willful blindness" or "deliberate ignorance"—should be covered so that management officials

1. Codified at 15 U.S.C. §§ 78dd-1(a).
2. 15 U.S.C. §§ 78dd-2(a), 78dd-3(a).
3. Codified at 15 U.S.C. § 78m(b)(2)(A).
4. Codified at 15 U.S.C. § 78m(b)(2)(B).
5. The FCPA further prohibits payments to foreign political parties and officials thereof.
6. *See* 15 U.S.C. §§ 78dd-1(a).
7. 15 U.S.C. §§ 78dd-1(f)(1).
8. *Id.*
9. *See* 15 U.S.C. § 78dd-1(f)(2)(B).

> could not take refuge from the Act's prohibitions by their unwarranted obliviousness to any action (or inaction), language or other "signaling [*sic*] device" that should reasonably alert them of the "high probability" of an FCPA violation.[10]

Since the 1977 enactment of the FCPA, the Anti-Bribery Provisions have applied to U.S. and foreign issuers of securities that registered their securities with or reported to the SEC and to domestic concerns such as U.S. citizens and companies organized under U.S. law or with a principal place of business in the United States, if the U.S. mails or a means or instrumentalities of U.S. interstate commerce (such as an interstate wire transfer) were used in furtherance of the anti-bribery violation.[11] In 1998, amendments to the Anti-Bribery Provisions generally extended U.S. jurisdiction to cover acts outside of U.S. territory in furtherance of an anti-bribery violation by U.S. issuers and domestic concerns and acts inside U.S. territory in furtherance of an anti-bribery violation by other persons, such as foreign non-issuers and foreign nationals, who were not previously subject to the FCPA.[12] Such extended jurisdiction is not dependent upon the use of U.S. mails or means or instrumentalities of U.S. interstate commerce.[13]

The FCPA also applies to officers, directors, employees, or agents of any organization subject to the FCPA and to stockholders acting on behalf of any such organization.[14]

B. The Exception and Defenses to Alleged Anti-Bribery Violations

Under the FCPA, facilitating payments "to expedite or to secure the performance of a routine governmental action" are excepted from the Anti-Bribery Provisions.[15] This is a narrow exception, only applying to non-discretionary acts such as obtaining official documents or securing utility service and not applying to any decision to award or continue business with a particular party.[16] Also, its practical effect is limited because many other jurisdictions and international conventions do not permit facilitation payments.

There are two affirmative defenses to the FCPA. Under the "written law" defense, it is an affirmative defense to an FCPA prosecution if the payment, gift, offer, or promise of anything of value that is at issue was lawful under the written laws and regulations of the recipient's country.[17] It is also an affirmative defense if the payment, gift, offer, or promise of anything of value was a reasonable, *bona fide* expenditure directly related either to the promotion, demonstration, or explanation of products or services, or to the execution or performance of a contract with a foreign government or agency.[18] Both defenses, however, are narrow in practice and, because they are affirmative defenses, it would be the defendant's burden to prove their applicability in the face of an FCPA prosecution.

10. H.R. Rep. No. 100-576, at 920 (1987) (Conf. Rep.), *reprinted in* 1988 U.S.C.C.A.N. 1547, 1953.
11. 15 U.S.C. §§ 78dd-1(a), 78dd-2(a).
12. 15 U.S.C. §§ 78dd-1(g), 78dd-2(i), 78dd-3(a).
13. *Id.*
14. 15 U.S.C. §§ 78dd-1(a), (g), 78dd-2(a), (i), 78dd-3(a).
15. 15 U.S.C. §§ 78dd-1(b), 78dd-2(b), 78dd-3(b).
16. 15 U.S.C. §§ 78dd-1(f)(3)(B), 78dd-2(h)(4)(B), 78dd-3(f)(4)(B).
17. 15 U.S.C. §§ 78dd-1(c)(1), 78dd-2(c)(1), 78dd-3(c)(1).
18. 15 U.S.C. §§ 78dd-1(c)(2), 78dd-2(c)(2), 78dd-3(c)(2).

C. Accounting Provisions

The FCPA's Accounting Provisions apply to issuers who have securities registered with the SEC or who file reports with the SEC.[19] The Books and Records Provisions compel such issuers to make and keep books, records and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer.[20] The Internal Accounting Controls Provisions require such issuers to devise and maintain a system of internal accounting controls regarding accounting for assets, enabling the preparation of financial statements, and providing reasonable assurances that management authorizes transactions and controls access to assets.[21] As used in the Accounting Provisions, "reasonable detail" and "reasonable assurances" mean a level of detail and degree of assurance as would satisfy prudent officials in the conduct of their own affairs.[22]

D. Penalties

The FCPA imposes both criminal and civil penalties. Willful violations of the Anti-Bribery Provisions carry maximum criminal fines of $2 million for organizations and $250,000 for individuals, per violation.[23] Under U.S. criminal law, alternative fines of up to twice the pecuniary gain from the offense apply instead, if the alternative fine exceeds the maximum fine under the FCPA.[24] Individuals also face up to five years' imprisonment for willful violations of the Anti-Bribery violations.[25] Anti-bribery violations also carry civil penalties of up to $16,000 for organizations or individuals, per violation.[26] These fines may not be paid by a person's employer or principal.[27]

Willful violations of the Accounting Provisions carry maximum criminal fines of $25 million for organizations and $5 million for individuals, or, if greater, the alternative fine of twice the pecuniary gain.[28] Individuals face up to 20 years' imprisonment for willful violations of the Accounting Provisions.[29] Civil penalties for violations of the Accounting Provisions include disgorgement of any ill-gotten gains and

19. 15 U.S.C. § 78m(b)(2). The Accounting Provisions were passed as part of the original 1977 FCPA legislation out of concern over companies improperly recording payments on their books and records and failing to fully account for illicit "slush" funds, from which improper payments could be made. These provisions, however, have broader application than simply within the context of the FCPA. For purposes of this Alert, when violations of these provisions are alleged in the context of improper payments to foreign officials or similar conduct, they are referred to as violations of the FCPA's Accounting Provisions. When violations occur in situations not involving improper payments (*see, e.g.*, the Willbros Group settlement discussed *infra*), they are described as the Exchange Act's books and records and/or internal controls provisions.
20. 15 U.S.C. § 78m(b)(2)(A).
21. 15 U.S.C. § 78m(b)(2)(B).
22. 15 U.S.C. § 78m(b)(7).
23. 15 U.S.C. §§ 78ff(c), 78dd-2(g), 78dd-3(e); 18 U.S.C. § 3571(b)(3), (e) (fine provision that supersedes FCPA-specific fine provisions).
24. 18 U.S.C. § 3571(d), (e) (fine provision that supersedes FCPA-specific fine provisions).
25. 15 U.S.C. §§ 78ff(c)(2)(A), 78dd-2(g)(2)(A), 78dd-3(e)(2)(A).
26. 15 U.S.C. §§ 78ff(c), 78dd-2(g), 78dd-3(e); *see* DOJ & SEC, A RESOURCE GUIDE TO THE FOREIGN CORRUPT PRACTICES ACT (2012) (indicating that the maximum civil penalty for an anti-bribery provision violation is $16,000, but citing the SEC's announcement of the adjustment for issuers subject to SEC enforcement without citing to a parallel DOJ announcement for domestic concerns and other persons).
27. 15 U.S.C. §§ 78ff(c)(3), 78dd-2(g)(3), 78dd-3(e)(3).
28. 15 U.S.C. § 78ff(a); 18 U.S.C. § 3571(d), (e).
29. 15 U.S.C. § 78ff(a).

penalties up to $775,000 for organizations and $160,000 for individuals, per violation, in actions brought by the SEC.[30]

II. Recent Policy Changes

A. Corporate Enforcement Policy

On November 29, 2017, Rod Rosenstein, the Deputy Attorney General, announced a new FCPA Corporate Enforcement Policy ("Policy"). The Policy, which was added to the U.S. Attorney's Manual at § 9-47.120, is designed to encourage corporations to voluntarily self-report in FCPA cases. It largely enacts the structure and requirements of the FCPA Enforcement Pilot Program (the "Pilot Program") announced by the DOJ in April 2016, but includes several notable distinctions.

Under the Policy, where a company has (1) voluntarily self-disclosed misconduct, (2) fully cooperated with the DOJ's ensuing investigation or follow-up questions, (3) taken sufficient remedial measures, including the adoption of an effective compliance program, and (4) agreed to pay all disgorgement, forfeiture, and/or restitution resulting from the misconduct, there will be a presumption that the company will receive a formal declination of prosecution, absent aggravating circumstances. If, given the circumstances, a criminal resolution is warranted but the company has met the four requirements listed above, the Policy states that the Fraud Section "will accord" a 50% reduction off of the otherwise-applicable U.S. Sentencing Guidelines penalty range, and generally will not require the appointment of a compliance monitor. Where a company is found not to have voluntarily self-disclosed its misconduct, but meets the other Policy requirements, the company will receive up to a 25% reduction off of the low end of the Sentencing Guidelines penalty range.

On July 25, 2018, Matthew Miner, the Deputy Assistant Attorney General who oversees the Fraud Section, clarified that the DOJ intends to apply the principles of the Policy to situations in which a successor company unearths FCPA violations post-acquisition—so long as the acquiring company discloses the issue to the DOJ and meets the other requirements of the Policy.

1. Elements of the FCPA Corporate Enforcement Policy

a. Voluntary Self-Disclosure

The cornerstone of the Policy is the requirement that a company voluntarily discloses the FCPA violation. In order for a disclosure to be considered voluntary, it must occur prior to an "imminent threat" of disclosure by an employee or third party or the initiation of a government investigation, must be made within a reasonable time of the company becoming aware of the violation, and must include all relevant facts (including information regarding the individuals involved). Notably, the Policy removed the restriction, previously included during the Pilot Program, that a disclosure is not considered voluntary if the company is required to make it by law, agreement, or contract.

30. 15 U.S.C. § 78u(d)(3), (5); *see* 17 C.F.R. § 201.1005, Table V (2013) (adjusting the amounts for inflation).

The Policy is clear that even with full cooperation and appropriate remediation, the Fraud Section's FCPA Unit will grant a maximum reduction of only 25% off the bottom of the U.S. Sentencing Guidelines penalty range if the company does not voluntarily disclose the misconduct.

b. Full Cooperation

In order to be eligible for the declination presumption, a company must also provide full cooperation to the DOJ's investigation. A company must be prepared to disclose all facts relevant to the misconduct and the company's internal investigation, including all facts that are known or become known regarding the involvement of the company's officers, employees, or agents in the criminal activity, as well as any facts regarding potential criminal conduct by third parties. Indeed, in many ways this requirement doubles down on the 2015 Yates Memorandum; in order to qualify for a declination or the reduced penalties available under the Policy, a company must be willing to name names.

In addition, the Policy details other steps that are required in order to receive credit for full cooperation:

- Preservation, collection and disclosure of relevant documents and information;
- Disclosure of overseas documents (unless the company can establish that disclosure is legally prohibited), including noting where the documents were found and by whom;
- Facilitation of third-party production of documents;
- Where requested, translation of relevant documents in foreign languages;
- Making available for DOJ interviews any company officers, employees, or agents who possess information relevant to the investigation—including those located overseas—as well as former officers and employees;
- Where possible, facilitating the production of witnesses by third parties;
- "De-confliction" of witness interviews and other investigative steps, when requested by the DOJ (i.e. deferring certain investigative steps at the request of the DOJ);
- Proactive cooperation (i.e. the company must disclose facts or opportunities to obtain evidence relevant to the investigation even absent a specific request from the DOJ);
- Updates on the status and findings of the company's internal investigation; and
- Disclosure of all relevant facts gathered during any independent investigation, including specifically an attribution of the sources of those facts rather than just a narrative.

The Policy is clear that the level of cooperation expected will be assessed based on the circumstances. A small company will not be required to conduct the same type of investigation (or in the same time frame) as a Fortune 100 company. However, a company will bear the burden of showing that its financial condition prevents it from providing more fulsome cooperation. Moreover, the Policy specifically states that full cooperation credit is not based on the willingness of the company to waive

attorney-client privilege or work-product protection. Finally, cooperation will not be assessed on an all-or-nothing basis; companies that meet some of the cooperation elements will be eligible for some cooperation credit under the Policy, but such credit will be "markedly less" than full cooperation credit.

c. Timely and Appropriate Remediation

A company must take timely and appropriate steps to remediate the misconduct, including conducting an analysis of the root causes of the underlying misconduct, implementing an effective ethics and compliance program, appropriately disciplining employees, and taking any other steps necessary to reduce the risk of misconduct recurring. The Policy includes a new requirement that remediation must include the appropriate retention of business records, including prohibiting employees from using "software that generates but does not appropriately retain business records or communications." This language appears to indicate that companies must instruct their employees not to use applications such as Telegram, Wickr, or a host of others, that can be set to (or which by default) automatically delete messages.

In order for a company to receive full credit for remediation and be eligible for a reduction in penalty under the Policy, the company must have effectively remediated the misconduct at the time of the resolution. Further, a company that does not cooperate will not be eligible for credit for remedial actions, though the effect of partial cooperation remains uncertain.

With respect to expectations regarding compliance programs, the Policy acknowledges that the implementation of an effective ethics and compliance program may vary depending on the size and resources of a company. However, the Policy provides several elements that the DOJ considers particularly important regardless of the size of the company:

- Whether the company has an overall culture of compliance, and an awareness among employees that any criminal conduct (including the conduct underlying the investigation) will not be tolerated;
- Whether the compliance function is independent and is granted sufficient resources;
- Whether the compliance function is staffed with quality and experienced compliance personnel, who are able to understand and identify the transactions posing potential risks;
- Whether the company has performed an effective risk assessment and tailored its compliance program to the risks identified in that assessment;
- How a company's compliance personnel are compensated and promoted compared to other employees;
- Whether the compliance program is monitored and audited to assure its ongoing effectiveness; and
- Whether the company has set up the reporting structure of compliance personnel in a manner that allows for independence and avoids potential conflicts of interest.

d. Disgorgement, Forfeiture, and Restitution

Finally, although not classified as a formal requirement, the Policy is clear that in order to qualify for a declination, a company is required to pay all disgorgement, forfeiture, and/or restitution resulting from their misconduct. In this context, the new Policy is more expansive than what was previously required by the Pilot Program. Under the Pilot Program, companies were required to "disgorge all profits resulting from *the FCPA violation*" (emphasis added). The new Policy requires companies to disgorge profits, as well as to pay any forfeiture or restitution, related to "*the misconduct at issue*" (emphasis added). This change leaves open the possibility that, in order to be eligible for a declination or reduction under the new Policy, companies may be required to pay disgorgement, forfeiture, or restitution related to misconduct identified during the investigation that goes beyond a violation of the FCPA.

2. Declination and Penalty Reduction

The most significant change from the Pilot Program to the Policy is the Policy's presumption of declination where a company has met the self-disclosure, cooperation, remediation, and disgorgement requirements outlined by the Policy. This presumption can only be overcome by the presence of "aggravating circumstances" involving either the seriousness of the misconduct or the profile of the offender. The Policy leaves significant room for prosecutorial discretion in determining what will be considered as an "aggravating circumstance" that would warrant a criminal resolution rather than a declination, but identifies several factors that may be sufficient:

- Involvement by the company's executive management in the misconduct;
- The company deriving "significant profit" related to the misconduct;
- The level of pervasiveness of the misconduct within the company; and
- Whether the company is a criminal recidivist.

The Policy does not include additional clarification on what fact patterns are sufficient to meet these circumstances. Questions, for example, about what level of profits are considered "significant," or about whether past non-FCPA settlements (or settlements by a subsidiary) mean that a company will be considered a recidivist, remain unanswered and may be purposely left to the discretion of prosecutors.

For companies which, based on aggravating circumstances, do not receive a criminal declination but otherwise fulfill the self-disclosure, cooperation, and remediation requirements, the Policy states that the DOJ "*will* accord, or recommend to a sentencing court" a 50% reduction from the low end of the U.S. Sentencing Guideline penalty range. This language has been strengthened from the guidance to the Pilot Program, which stated that in such circumstances the Fraud Section "*may* accord" up to a 50% penalty reduction. This change indicates the DOJ's desire to provide additional certainty to companies about the benefits they will receive through self-disclosure and cooperation.

Finally, the Policy indicates that, for companies that qualify for the 50% reduction, the DOJ will generally not require the appointment of an independent compliance monitor, so long as the company has implemented an effective compliance program at the time of the resolution (as evaluated while considering remediation credit).

Companies that do not voluntarily disclose their misconduct to the DOJ, but which later provide full cooperation and meet the Policy's standards for remediation can receive a lower level of penalty reduction. The Policy states that in these circumstances the company "*will* receive" up to a 25% reduction off of the low end of the U.S. Sentencing Guidelines penalty range. Due to the Policy's definition of the circumstances in which a disclosure is considered "voluntary," a company that makes a self-disclosure to the DOJ may find itself eligible for only a 25% reduction in penalty if, at the time of its disclosure, the DOJ was already aware of the misconduct, or if the DOJ determines that the company faced the "imminent threat" of the initiation of a government investigation (for example, due to prior media reports).

3. Application beyond FCPA Matters

Although explicitly designed for FCPA cases, the DOJ has indicated that the Policy may have more expansive application. On March 1, 2018, John Cronan, then-Acting Assistant Attorney General for the DOJ's Criminal Division, and Benjamin Singer, Chief of the Fraud Section Securities and Financial Fraud Unit, announced that the DOJ's Criminal Division would apply the Policy as nonbinding guidance in cases that do not involve FCPA violations.

Cronan and Singer highlighted the example of the DOJ's February 2018 declination to prosecute Barclays PLC for misconduct related to front-running foreign exchange transactions by one of its clients, based on Barclays's voluntary self-disclosure, comprehensive investigation, full and continuing cooperation, compliance program enhancements, and payment of $12.9 million in restitution and disgorgement. They contrasted this result with the January 2018 DPA in which HSBC agreed to pay $101.5 million in criminal penalties and disgorgement to resolve charges related to a similar front-running scheme, noting that HSBC did not self-report its misconduct and, at least initially, was not fully cooperative with the DOJ.

4. Declinations under the Pilot Program and Corporate Enforcement Policy

In announcing the Policy, Deputy Attorney General Rosenstein presented it as a continuation of and an improvement upon the Pilot Program. He described the Pilot Program as a success, noting that the DOJ's FCPA Unit received 30 voluntary disclosures during the 18 months in which the Pilot Program was in effect, compared with 18 during the previous 18-month period. Over the course of the Pilot Program, the DOJ did demonstrate a willingness to decline to prosecute companies that fully meet its requirements, at least for conduct that was neither egregious nor widespread. During that time, the DOJ published seven declination letters (Nortek, Akamai, Johnson Controls, HMT LLC, NCH Corporation, Linde, and CDM Smith), each referencing the Pilot Program. These cases all involved relatively small value bribes or other benefits provided to government officials, and each company either reached some sort of settlement with the SEC related to the underlying misconduct or agreed to pay disgorgement as part of the declination itself.

The Policy states that the DOJ will make public any declinations made pursuant to the Policy—that is any case that would have been prosecuted or criminally resolved but for the company's compliance with the Policy requirements of disclosure, cooperation, remediation, and disgorgement. Since the Policy's release, several declination letters have been made available on the DOJ's website; several additional companies have made SEC filings claiming that they received declination letters which

have not been published (i.e. Teradata (February 20, 2018) and Exterran (February 28, 2018)). Given the conditions governing the circumstance in which the DOJ has committed to publish its declination letters, it seems likely that these declinations were made not based on the relevant companies' voluntary disclosure under the Policy, but instead due to some other concerns (i.e. jurisdictional, evidentiary, or statute of limitations issues).

Several recent declinations which were issued pursuant to the Pilot Program or under the new Policy, and which were published on the DOJ website, are described below.

a. Linde North America Inc. and Linde Gas North America LLC

On June 16, 2017, the DOJ issued a declination letter to Linde North America Inc. and Linde Gas North America LLC (collectively, "Linde"), and certain of Linde's subsidiary companies and affiliates, in connection with alleged violations of the FCPA's anti-bribery provisions. According to the DOJ, beginning in November 2006, Spectra Gases, Inc. ("Spectra Gases"), a Linde subsidiary, made illegal payments to officials of the Republic of Georgia ("Georgia") in exchange for the officials' selection of Spectra Gases as the purchaser of industrial equipment. The DOJ required Linde to disgorge all profits it had earned from the arrangement, which totaled $7.82 million, and to forfeit $3.415 million in "corrupt proceeds" it owed to public officials of Georgia under the illegal arrangement.

In October 2006, Linde acquired Spectra Gases, a New Jersey company. Spectra Gases' three primary shareholders and managers (the "Spectra Executives") continued to work for the company for three years after the acquisition under a so-called "earn-out" arrangement. According to the DOJ, they also continued to operate a bribery scheme they had set in motion before Linde acquired their company. Under the scheme, high-level officials at Georgia's state-owned National High Technology Center ("NHTC") agreed to help ensure that Spectra Gas subsidiary, Spectra Investors, LLC ("Spectra Investors") was chosen as the purchaser of certain industrial assets, including a boron column for producing boron gas. The parties then set up a subsidiary and shell companies and entered into an apparently fictitious "management agreement" to compensate the NHTC officials for their assistance.

Ultimately, the NHTC officials received a 51% ownership stake in Spectra Investors, and took roughly 75% of the earnings generated by the boron column. Linde earned profits from the arrangement totaling $7.82 million, including $6.39 million from the inception of the scheme through December 2009—at which point Linde dissolved Spectra Gases as an entity—and a further $1.43 million from January 2010 until the unspecified date the scheme came to a halt. When it discovered the bribery, Linde withheld $10 million in the Spectra Executives' "earn-out" fees, as well as additional payments to be made to NHTC officials through companies they owned or controlled.

The DOJ cited the FCPA Pilot Program as the basis for its declination letter. It pointed to several factors that influenced its decision not to prosecute, such as Linde's:

- Timely and voluntary disclosure;
- Extensive and proactive internal investigation;
- Full cooperation, which included providing all facts it knew about relevant individuals;

- Agreement to disgorge the profits it earned from illegal activity and forfeit funds it would have owed to NHTC officials under the scheme;
- Previous and continuing enhancement of its compliance program; and
- "[f]ull remediation," which included terminating or otherwise disciplining both the Spectra Executives and lower-level employees involved in the scheme, terminating its apparently fictitious "management agreement" with a company owned by NHTC officials, and withholding payments slated for the Spectra Executives and NHTC officials.

b. CDM Smith

On June 21, 2017, the DOJ issued a declination letter to CDM Smith Inc. ("CDM Smith"), a private Massachusetts engineering and construction company, in connection with alleged violations of the FCPA's anti-bribery provisions. According to the DOJ, CDM Smith paid approximately $1.18 million in bribes to government officials in India to secure public works contracts. The contracts netted CDM Smith $4,037,138 in profit, which it is required to disgorge as a condition of the DOJ's decision not to prosecute.

From roughly 2011 until 2015, as described in the declination letter, employees and agents of CDM Smith and its Indian subsidiary ("CDM India") bribed public officials working at the National Highways Authority of India ("NHAI") via pass-through subcontractors. In exchange for a 2-4% kickback, NHAI officials helped CDM Smith and CDM India secure contracts for highway design and construction supervision. Employees of CDM Smith and CDM India also allegedly bribed public officials in the Indian state of Goa in connection with a water project contract. The DOJ found that "[a]ll senior management at CDM India" not only knew of the misconduct, but approved of it or even participated in it directly.

The DOJ cited the FCPA Pilot Program as the basis for its declination letter. It pointed to several factors that influenced its decision not to prosecute, such as CDM Smith's:

- Timely and voluntary disclosure;
- Extensive internal investigation;
- Full cooperation, which included providing all facts it knew about the individuals connected to the scheme;
- Agreement to disgorge the profits it earned from illegal activity;
- Previous and continuing enhancement of its compliance program; and
- "[f]ull remediation," which included terminating all employees and executives who took part in or orchestrated the misconduct.

c. Dun & Bradstreet

On April 23, 2018, the DOJ issued a declination letter to The Dun & Bradstreet Corporation. ("Dun & Bradstreet"), a then-publically traded New Jersey commercial data company, in connection with alleged violations of the FCPA's anti-bribery provisions. The DOJ's declination letter was issued on the same day

that the SEC announced a settlement with Dun & Bradstreet, under which Dun & Bradstreet agreed to pay approximately $9.2 million, including $6.1 million in disgorgement, $1.1 million in prejudgment interest, and a $2 million civil penalty in order to resolve charges related to improper activities in China.

In 2012, Dun & Bradstreet learned that, from 2006 to 2012, two of its Chinese subsidiaries made payments to third-party agents as well as to Chinese government officials in order to obtain non-public business and personal information relevant to Dun & Bradstreet's business model as a provider of financial information. Prior to its acquisition of each subsidiaries, Dun & Bradstreet's pre-acquisition due diligence raised concerns regarding the methods employed by the acquisition target to obtain data. Nonetheless, in both cases Dun & Bradstreet proceeded with the acquisition, and did not take sufficient action post-acquisition to prevent the improper payments or to avoid improper entries in its books and records.

The DOJ cited the Policy as its basis for declining prosecution. It listed a number of factors which influenced its decision not to prosecute, including that Dun & Bradstreet:

- Identified the misconduct and made a "prompt voluntary self-disclosure";
- Conducted a thorough investigation and cooperated fully, including identifying all individuals involved in or responsible for the misconduct;
- Made current and former employees available for interviews;
- Voluntarily produced and translated foreign documents;
- Enhanced its compliance program and internal accounting controls;
- Demonstrated its full remediation by terminating 11 employees involved in the misconduct and disciplining others by reducing salaries, bonuses, and performance reviews; and
- Made a full disgorgement to the SEC.

d. ICBL

On August 23, 2018, the DOJ issued a declination letter to Insurance Corporation of Barbados Limited ("ICBL"), a Barbados-based insurance provider, in connection with alleged violations of the FCPA's anti-bribery provisions. According to the DOJ, ICBL paid approximately $36,000 in bribes to a Barbados public official, in exchange for assistance in securing two government contracts. ICBL also assisted the public official in laundering the funds through accounts held in the United States. The contracts resulted in $93,940.19 in profits for ICBL, which it was required to disgorge as a condition of the DOJ's declination of prosecution.

From 2015-2016, as described in the declination letter, senior employees of ICBL participated in a scheme to make payments to an individual who was then a sitting member of the Barbados Parliament, as well as the country's Minister of Industry, International Business, Commerce, and Small Business Development. This individual used his position to direct government contracts to ICBL. The company assisted the public official's efforts to conceal the bribes by making payment to a U.S. bank account held

in the name of a business owned by a friend of the official, who then transferred the funds on to the official's U.S. bank account.

Although the DOJ noted the involvement of high-level ICBL employees in the misconduct, it elected to close its investigation into the matter and to decline to prosecute the company based on ICBL's:

- Timely and voluntary self-disclosure;
- Comprehensive investigation;
- Cooperation with the DOJ by providing all known facts regarding the misconduct, and commitment to continue to cooperation in the DOJ's ongoing investigations and prosecutions;
- Agreement to disgorge all profits resulting from the misconduct;
- Enhancements made to its compliance program and internal accounting controls;
- Remedial actions, including the termination of all employees and executives involved in the misconduct; and
- The DOJ's success in identifying and bringing charges against the culpable individuals.

B. Piling On

On May 9, 2018, Deputy Attorney General Rod Rosenstein announced a new Department of Justice (DOJ) policy, to be incorporated into the U.S. Attorneys' Manual, discouraging the practice of "piling on" — imposing excessive or redundant penalties — in corporate enforcement actions. The policy instructs DOJ attorneys to coordinate with attorneys in other DOJ components that are investigating the same corporate misconduct, and with other domestic and foreign enforcement agencies (when possible), to achieve equitable results. In announcing the policy, Rosenstein explained that it strives to "ensure that corporate resolutions that flow from parallel or joint investigations into the same conduct are reasonable and proportionate to that conduct." The new policy articulates the emerging practice by DOJ but is careful in the flexibility it affords DOJ in determining when multiple penalties will be deemed appropriate.

The policy responds to the growing reality that businesses operate in multiple jurisdictions and are accountable to multiple domestic and foreign regulatory bodies. "That creates a risk," explained Rosenstein, "of repeated punishment that goes beyond what is necessary to rectify the harm and deter future violations."

The policy has four main components:

- First, it reaffirms that the federal government's criminal enforcement authorities should not be used to extract larger civil settlements.

- Second, the policy directs components within DOJ seeking to resolve a case based on the same misconduct to coordinate with one another in order to achieve equitable results.

- Third, the policy encourages DOJ attorneys, when possible, to coordinate with other federal, state, local, or foreign enforcement authorities investigating a company for the same misconduct.

- Fourth, the policy articulates factors to guide the determination of whether multiple penalties serve the interests of justice in a particular case. These factors include (1) the egregiousness of the wrongdoing; (2) statutorily mandated penalties; (3) the risk of delay in finalizing a resolution; and (4) the adequacy and timeliness of a company's disclosures and cooperation with DOJ.

III. FCPA Settlements and Enforcement Actions[31]

A. 2018[32]

1. Beam Inc.

On July 2, 2018, Beam Inc. (*a.k.a.* Beam Suntory Inc., "Beam") agreed to pay approximately $8.2 million to resolve claims that it violated the books and records and internal controls provisions of the FCPA through the actions of its Indian subsidiary. Without admitting or denying the SEC's allegations, Beam consented to the entry of a cease and desist order ("Order"), which details improper payments by Beam's Indian subsidiary from approximately 2006 through 2012.

Headquartered in Chicago, Illinois, Beam is a beverage and spirits company, most famous for its Jim Beam brand bourbon. During the relevant time period, a class of Beam Inc.'s securities was publicly traded on the New York Stock Exchange. In April 2014, Suntory Holdings Limited acquired Beam Inc. and Beam Inc. delisted from the NYSE. From that point, Beam operated in the name of Beam Suntory Inc. Beam's Indian subsidiary, Beam Global Spirts & Wine (India) Private Limited ("Beam India"), was acquired in 2006. Beam India's books and records were consolidated into that of Beam's and reported by Beam on its financial statements.

Beam India bottled and sold Beam products in India, where the alcoholic beverage industry is subject to heavy government regulations, covering importation of alcoholic products, shipment between bottling facilities and distribution warehouses, label registration, warehouse licensing prior to retail distribution, and sales to retail stores operated by the Indian government. Through third-party promoters, Beam India allegedly made improper payments to government officials to promote the sale of Beam products at government-owned retail stores and to facilitate regulatory processes such as facilities

31. Hughes Hubbard represents or has represented multiple companies who have been the subject of the enforcement actions or other activities summarized in this Alert. All details and information provided in this Alert in connection with such enforcement actions, however, are based solely on the government's charging documents or other publicly available documents. Additionally, all descriptions of allegations underlying the settlements (or other matters such as ongoing criminal cases) discussed in this Alert are not intended to endorse or confirm those allegations, particularly to the extent that they relate to other, non-settling entities or individuals.
32. Cases and settlements have been organized alphabetically within each year.

inspection and annual label registration. To conceal the illicit payments, the SEC alleged that third-party promoters issued inflated or fabricated invoices to Beam India, which were falsely characterized in Beam India's books and records as legitimate business expenses such as "Customer Support" or "Off-Trade Promotions."

Beam India also allegedly made payments to government officials to obtain or accelerate registration, inspection, and licensing requirements. For example, in 2011, to accelerate a label application that had been stalled for months, Beam India allegedly paid a senior excise official a total of one million Indian Rupees ($18,000 at the then exchange rate) through a third-party bottler. The third-party bottler allegedly submitted two false invoices in the approximate amount of the payment, for the purpose of "consulting services rendered at the bottling facility."

According to the SEC, beginning in January 2011, Beam began to receive information calling into question the practices of Beam India. A report of a global accounting firm that had been retained to conduct a compliance review of Beam India noted that certain executives of Beam India believed that promoters may be making grease payments to Indian government officials. Over the course of the next year, Beam continued to receive indications of its risks in India, including the July 2011 news of FCPA violations in India by Beam's direct competitor, Diageo plc, in July 2011. Although Beam took certain steps to address the problems, the SEC alleged that Beam did not take full remedial measures until whistleblower reports and another compliance reports led to an internal investigations in September 2012.

Beam's $8.2 million settlement consists of disgorgement of profit in the amount of $5,264,340, prejudgment interest of $917,498, and a civil monetary penalty of $2,000,000. In reaching the settlement, the SEC noted Beam's failure to timely remediate the deficiencies in its FCPA compliance and internal controls. On the other hand, the SEC acknowledged Beam's voluntary disclosure of the misconduct, cooperation in producing relevant documents and findings, and remedial actions taken in a timely manner following its internal investigation. Beam's remedial measures included ceasing business operation at Beam India until satisfaction of its compliance operation, terminating Beam India employees involved in the misconduct, terminating third-party promoters in India, and enhancing its anti-corruption compliance procedures on a global basis, with an emphasis on third-party due diligence.

Along with Diageo and Anheuser Busch InBev, Beam is at least the third beverage company that has resolved FCPA allegations based, at least in part, on improper payments made to officials involved in the regulation and sale of alcoholic beverages in India.

2. Credit Suisse

In May and July 2018, Credit Suisse Group AG ("Credit Suisse") and its subsidiary, Credit Suisse (Hong Kong) Limited ("Credit Suisse HK") agreed to pay approximately $76.7 million in penalties and disgorgement to resolve investigations by the DOJ and SEC into Credit Suisse's illicit referral hiring program in the Asia-Pacific region, which, according to the DOJ and SEC, violated the FCPA's internal controls and anti-bribery provisions.

Credit Suisse is a Switzerland-based corporation with numerous subsidiaries, affiliated companies, and branches around the globe. At all relevant times, its shares were publically traded on the New York Stock Exchange, qualifying Credit Suisse as an "issuer" under the FCPA. Credit Suisse HK is

a wholly-owned, Hong Kong-registered subsidiary of Credit Suisse that offers securities products and financial advisory services under the Credit Suisse brand in the Asia-Pacific Region. Under the FCPA, Credit Suisse HK constituted an "agent" of issuer Credit Suisse.

a. Referral Hiring Program

The SEC and DOJ alleged that between 2007 and 2013, Credit Suisse HK provided employment to more than 100 relatives and friends referred by or connected to Chinese government officials ("referral hires") in order to obtain or retain investment banking business from Chinese state-owned enterprises and regulatory approvals from government agencies. Senior managers in Hong Kong repeatedly engaged in such practices to improperly influence Chinese government officials in explicit and knowing violation of Credit Suisse's anti-corruption policies against the *quid pro quo* hiring of government officials and their relatives. Credit Suisse HK senior managers designated some referral hires as "must hire" despite the fact that the candidates did not meet Credit Suisse's hiring standards and instructed subordinate employees to inflate the candidates' interview ratings. To track how referral hires' relationships to government officials "translated" into business opportunities, Credit Suisse HK maintained spreadsheets linking each referral hire to the business or approval granted by the related SOE or agency.

The DOJ and SEC outlined numerous instances where Credit Suisse HK managers communicated in emails the need to hire, promote, or compensate otherwise unqualified individuals to secure business. For example, Referral Hire A, the daughter of a high-ranking official at a Chinese SOE ("SOE A"), was hired in 2010 according to instructions from a Credit Suisse HK Vice President and a senior investment banking manager. Referral Hire A was rushed through the hiring process because she was "a princess" and because her hiring would allow Credit Suisse HK to "push her mum" and "get [Credit Suisse HK] in the deal." To accomplish this, Credit Suisse HK employees even created a new resume for her to make her application more presentable. Referral Hire A was hired only six days after Credit Suisse HK received her resume, and the next month, Credit Suisse HK was awarded business by one of SOE A's subsidiaries that earned $950,000 in fees. Until Referral Hire A's resignation in May 2015, Credit Suisse HK regularly promoted Referral Hire A despite her poor performance because of the business awarded to Credit Suisse HK by her mom. In total, Referral Hire A collected more than $1 million in compensation from Credit Suisse HK between 2010 and 2015.

In another example included in the charging documents, Referral Hire B was referred to Credit Suisse HK by Foreign Official B, a high-ranking official at another Chinese SOE. In December 2007, Referral Hire B was offered a three-month internship in Shanghai and, at the request of Foreign Official B, was offered a full-time position in Hong Kong in March 2008. In May 2008, Credit Suisse was selected as the bookrunner for the IPO of the subsidiary of the Chinese SOE and as financial advisor on an M&A transaction for the Chinese SOE. These two mandates earned approximately $21.3 million for Credit Suisse HK. During the 2008 financial crisis, Credit Suisse HK senior managers eliminated highly-rated analysts in favor of keeping Referral Hire B because of the promise of forthcoming "relationship revenue" from Referral Hire B. In March 2009, the Chinese SOE awarded Credit Suisse a mandate that generated $1.18 million in revenue. In several other instances, Credit Suisse's inclusion of Referral Hire B on a deal team or Referral Hire B's personal communications with Foreign Official B were sufficient to secure Credit Suisse a role in an upcoming deal.

b. Resolution of the Allegations

On May 24, 2018, Credit Suisse HK entered into a non-prosecution agreement with the DOJ related to the hiring scheme. Credit Suisse HK and Credit Suisse agreed to pay a $47 million criminal penalty and to continue cooperating with the DOJ in its investigation relating to the conduct. On July 5, 2018, Credit Suisse agreed to pay disgorgement of $24.9 million and $4.8 million in interest to the SEC. The SEC stated that it took the criminal penalty from the DOJ into consideration in deciding that it would not impose any civil penalties. While the DOJ did not require the appointment of a compliance monitor, Credit Suisse HK and Credit Suisse agreed to report at least once every 12 months over a period of three years regarding ongoing remediation efforts and the implementation of a strengthened compliance program at Credit Suisse HK and Credit Suisse.

The criminal penalty against Credit Suisse HK represented a 15% discount off the low end of the U.S. Sentencing Guidelines fine range. Credit Suisse HK received credit for its (and Credit Suisse's) cooperation with the DOJ's investigation, including voluntarily making foreign-based employees available for interviews in the US and providing translations of foreign language documents. The DOJ did not award the full 25% reduction to which Credit Suisse HK may have been eligible because, according to the DOJ, Credit Suisse HK failed to sufficiently discipline employees who engaged in the misconduct.

3. Dun & Bradstreet

On April 23, 2018, the SEC filed a cease-and-desist order against Dun & Bradstreet Corporation ("D&B") for alleged violations of the FCPA's accounting and internal controls provisions. D&B, a publicly-traded Delaware company based in New Jersey, is a global provider of business information, and it conducts reporting of credit and commercial data on millions of companies. According to the SEC, from 2006 to 2012, two of D&B's indirect subsidiaries in China, Shanghai Huaxia Dun & Bradstreet Business Information Consulting Co., Limited ("HDBC") and Shanghai Roadway D&B Marketing Services Co., Ltd. ("Roadway"), made improper payments to government officials and Chinese SOEs in order to obtain or retain business.

Without admitting or denying the SEC's allegations, D&B agreed to disgorge profits of $6,077,820 and pay $1,143,664 in prejudgment interest. Additionally, D&B agreed to pay a civil penalty in the amount of $2 million.

The DOJ issued D&B a formal declination under the FCPA Corporate Enforcement Policy (*see* p. 10).

a. Alleged Misconduct

i. HDBC Joint Venture

In 2006, through D&B's Chinese subsidiary, Dun & Bradstreet International Consultant (Shanghai) Co. Ltd. ("D&B China"), D&B formed the joint venture HDBC with Huaxia International Credit Consulting Co. Limited ("Huaxia"). D&B China owns 51% of HDBC.

According to the SEC, D&B performed due diligence on Huaxia before the formation of HDBC, which revealed that Huaxia relied on its government connections to source non-public and restricted

information directly from various government agencies, including the State Administration of Industry and Commerce. While D&B's senior managers were reportedly aware that Huaxia routinely made improper payments to government officials in exchange for information, D&B failed to adequately address the issue. Instead, D&B merely provided a short FCPA training to Huaxia executives and requested that they to complete anti-bribery questionnaires and certifications.

The SEC further alleged that after HDBC was established, D&B stopped Huaxia employees' practice of making direct payments to Chinese government officials in exchange for confidential information and began using third-party agents to achieve the same goal. D&B reportedly took this approach under the mistaken belief that using third parties would shield the company from legal liability, and the tactic made data acquisition costs in China significantly higher than similar costs in other countries. In 2008, D&B considered eliminating the use of third parties and instructing HDBC employees to purchase data directly from government officials. However, employees responsible for data and operations at HDBC allegedly reported that direct purchases would require "lots of palm grease." The Order alleges that D&B was also concerned that it could not obtain tax receipts if it purchased information directly from officials. In the end, D&B allegedly opted to continue using third parties to provide illicit payments to government officials in order to gain advantages for HDBC, a practice that did not end until 2012.

ii. Roadway

Roadway was a direct marketing services company in China that purchased much of its data from third-party vendors. In June 2009, D&B acquired 90% of Roadway through a wholly owned subsidiary. D&B reportedly conducted pre-acquisition due diligence on Roadway. During this due diligence, Roadway reportedly refused to warrant that its sales force did not pay kickbacks to decision-makers to "drum up" business. Despite this clear red flag, D&B allegedly failed to further investigate whether Roadway acquired its data by any illegal means, or whether the company's sales force was paying bribes to government officials.

After the acquisition, Roadway continued its practice of purchasing consumer data from third parties. D&B was satisfied with certifications from those third parties stating that the data was legally obtained, although D&B allegedly did not audit or review the sources of the data purchased, or otherwise verify whether the data was obtained legally.

D&B also allegedly failed to verify whether Roadway employees were making improper payments to customer decision-makers. According to the SEC, from July 2009 to March 2012, Roadway employees made improper payments disguised as "promotional expenses" to customers in order to obtain or retain business, including payments to Chinese government agencies and SOEs. These "promotional expenses" were provided to customers both through agents and by Roadway employees directly. During the relevant period, 34% percent of customer transactions involved such "promotional expenses," which covered over a thousand customers, including 156 Chinese government agencies and SOEs.

On March 15, 2012—China's National Consumer Protection Day—a Chinese news program revealed the existence of Roadway's extensive databases of citizen information, which included "specific financial, employment, and contact information that Roadway sold to companies for marketing purposes." Police in Shanghai raided Roadway's headquarters the same day, confiscating electronic databases and

detaining individuals involved with Roadway's data acquisition operations. In September 2012, the Chinese government charged Roadway with illegally obtaining private information of citizens and ordered the company to pay a $160,000 criminal fine.

b. Resolution

The Order states that illicit payments by HDBC and Roadway were falsely recorded as legitimate business expenses, which were consolidated in D&B's books and records. Furthermore, the Order alleges that despite concerns raised during pre-transaction due diligence, D&B failed for several years to develop and maintain a sufficient system of internal controls to prevent and detect improper payments in data acquisitions and sales. The SEC consequently charged D&B with violations of the FCPA's accounting and internal control provisions.

On April 23, 2018, the DOJ issued D&B a formal declination under the FCPA Corporate Enforcement Policy. The DOJ stated that it had reached this decision "despite the bribery committed by employees of the [c]ompany's subsidiaries in China" based on a number of factors. These included: prompt and voluntary self-disclosure; thorough internal investigation; full cooperation with authorities, including identifying responsible individuals, providing the DOJ with all relevant facts, making both current and former employees available for interviews, and translating documents to English as necessary; full remediation, including terminating 11 employees involved in the misconduct and disciplining others with financial sanctions and formal reprimands; and agreement to disgorge the improper profits in full to the SEC.

4. Elbit Imaging Limited

On March 9, 2018, the SEC filed a cease-and-desist order against Elbit Imaging Ltd. ("Elbit") related to its findings that Elbit had violated the FCPA's books and records and internal accounting controls provisions in real estate projects in both Romania and the United States. According to the SEC, Elbit and its subsidiary, Plaza Centers NV ("Plaza"), made payments to two third-party consultants and a sales agent without evidence that these third parties provided actual services. Elbit consented to the order without admitting or denying the SEC's findings and agreed to pay a $500,000 civil penalty in order to settle the FCPA violations.

Elbit is headquartered in Petach Tikva, Israel. An international holding company, Elbit owns subsidiaries in various industries, including real estate development. Plaza is a Netherlands corporate entity that focuses on constructing and modernizing "Western-style" shopping and entertainment centers in Central and Eastern Europe. Plaza was at the time of the relevant conduct majority-owned and controlled by Elbit and its financial statements were consolidated into Elbit's financial statements.

Until February 2014, Elbit's then-CEO, Mordechai (Moti) Zisser held majority ownership in Elbit. Moti Zisser also served as Plaza's Executive Director until February 2014.

a. Casa Radio Project

In 2006, Plaza sought to participate in the Casa Radio Project, a large real estate development project located in Bucharest, Romania. Plaza engaged two third-party consultants, one in 2006 (the "2006 Consultant") and one in 2011 (the "2011 Consultant"). Both consultants were offshore entities allegedly

retained at Mr. Zisser's direction. The SEC found no evidence to suggest that Plaza conducted any pre-engagement due diligence on either consultant.

The 2006 Consultant was nominally hired to, among other tasks, provide consulting services and assistance in obtaining government approvals for the development project. In February 2007, Plaza purchased a 75% interest in the Casa Radio Project for $40 million and a commitment to finance and develop a Romanian public authority building. The SEC found no evidence that the 2006 Consultant provided any services in connection to this transaction.

The 2011 Consultant was similarly hired to assist Plaza in securing governmental approvals and to assist Plaza in purchasing from the Romanian government an additional 15% interest in the Casa Radio Project. Although Plaza successfully acquired the 15% interest in the project, the SEC found no evidence that the 2011 Consultant had provided any services in relation to this acquisition.

In total, Plaza, directly or indirectly, paid the 2006 and 2011 Consultants approximately $14 million from 2007 through 2012. Plaza senior officers authorized these payments despite the absence of requisite documentation to support the payments. Additionally, Plaza categorized these expenses in its books as legitimate business expenses for services rendered. In its findings, the SEC alleged that some or all of the funds may have been used to make corrupt payments to Romanian officials or were simply embezzled.

b. U.S. Real Estate Portfolio Sale

In late 2011, a joint venture of investors (the "Joint Venture"), of which Elbit and Plaza together held a 45.4 percent stake, sought to sell a portfolio of 47 shopping center real estate assets in the United States (the "Portfolio"). The Joint Venture hired a financial advisor (the "JV advisor") to assist the Joint Venture in selling these assets. The JV advisor ultimately received $6.75 million for services rendered in relation to the June 2012 sale of the Portfolio.

In November 2011, approximately six weeks after the Joint Venture retained the JV advisor, Elbit and Plaza entered into a sales agency agreement with an offshore entity ("Sales Agent A"), for the stated purpose of assisting Elbit and Plaza in selling the Portfolio. Sales Agent A was not hired by the Joint Venture and Elbit and Plaza did not conduct any due diligence on Sales Agent A. Under Sales Agent A's contract with Elbit and Plaza, Sales Agent A was responsible for creating marketing materials, locating potential buyers, and assisting in negotiating a sales contract, services which largely mirrored those for which the JV advisor had already been retained. In exchange, Sales Agent A would receive a success fee totaling 0.9% of the Portfolio's gross sale price.

The day after Elbit and Plaza executed the sales contract with Sales Agent A, Sales Agent A subcontracted with another offshore entity ("Sales Agent B"), assigning all of its rights and responsibilities under the Sales Agent Agreement to the second entity. Mr. Zisser indirectly owned Sales Agent B, which was to receive approximately 98% of remuneration due to Sales Agent A under this subcontract. Mr. Zisser did not disclose his interest in Sales Agent B, and Elbit and Plaza were not aware that Sales Agent A had subcontracted with this entity.

The Joint Venture sold the Portfolio on June 21, 2012, for $1.428 billion. Following the sale, Elbit and Plaza paid Sales Agent A $13 million, or almost double the commission paid to the JV advisor. The $13 million was nominally for Sales Agent A's commission and expenses and was paid despite the absence of requisite proofs of services rendered. Sales Agent A in turn paid Sales Agent B $12.75 million. Only Mr. Zisser was aware of this remuneration scheme. In its investigation of these payments, the SEC did not identify any evidence showing that either Sales Agent A or Sales Agent B had provided services related to this agreement.

c. Resolution

Elbit and Plaza self-reported to the Romanian and U.S. authorities following Elbit's discovery of information suggesting that payments made by Plaza in relation to the Casa Radio Project may have been improper and incorrectly recorded in Plaza's books and records. Elbit, through a special committee of its board of directors, retained outside counsel to conduct an independent investigation. While the investigation was being conducted, additional information came to light regarding Elbit and Plaza's payments to Sales Agent A and Sales Agent B's ownership. This new information led Elbit and Plaza to form a joint special committee to review the Portfolio sale. Elbit shared its external counsel's findings with the SEC, including providing translations of certain documents, and was responsive to the SEC's requests for additional information.

The SEC determined that Elbit and Plaza's internal accounting controls failed to identify that payments of $27 million were made to the 2006 Consultant, 2011 Consultant, and Sales Agent A with little or no indication that these parties had actually provided services justifying this remuneration. The SEC noted in particular that Plaza's legal department had limited involvement in, and oversight over, Plaza's contracts with third-party agents and consultants. These deficiencies in Plaza's internal controls led to inaccuracies in Elbit's books and records. Finally, neither Elbit nor Plaza maintained policies and procedures aimed at detecting corruption risks or training employees on anti-corruption compliance. In agreeing to the settlement, the SEC positively cited Elbit and Plaza's self-reporting to the authorities, implementation of "extensive" remedial measures, and full cooperation with the SEC investigation alongside a thorough internal investigation. It additionally noted that Elbit was in the process of selling its principal assets in order to service its debt obligations and was not developing current or new business.

5. Kinross Gold

On March 26, 2018, the SEC entered a cease-and-desist order against Kinross Gold Corp. ("Kinross"), a NYSE-listed gold mining company based in Toronto, to settle allegations that Kinross violated the FCPA's books and records and internal controls provisions. Without admitting or denying the allegations, Kinross agreed to a yearlong reporting of its remedial steps and a $950,000 civil penalty for failing to devise and maintain proper internal accounting controls post-acquisition of two mining operations in Africa, despite identifying accounting and compliance failures during the pre-acquisition stage.

On November 7, 2017, the DOJ informed Kinross that it was declining to prosecute the same conduct.

According to the SEC, in September 2010, Kinross acquired two African mining operations and associated assets: Tasiast Mauritanie Limited S.A. ("Tasiast") in Mauritania and Chirano Gold Mines Ltd ("Chirano") in Ghana, from Vancouver-based Red Back Mining, Inc. ("Red Back"), for $7.1 billion. During pre-acquisition due diligence, Red Back disclosed its lack of anti-corruption and internal accounting controls surrounding its contractual, procurement, petty cash, and vendor payment processes. Following the acquisition, Kinross failed to timely implement sufficient internal accounting controls and remediate known issues, including the use of petty cash by low-level employees to pay vendors and the lack of due diligence on vendors.

In April 2011, Kinross' internal audit reported that the accounting and disbursement (Enterprise Resource Planning ("ERP")) systems at both mining operations contained insufficient details on the nature of disbursements, making it "not possible" to identify suspect payments such as excessive rebates and discounts, advance payments, government commissions, and unjustified business expenses. In addition, internal audit also found that the two mines did not maintain proper tendering and contracting processes. Kinross management, however, failed to remediate these issues. In 2012, at the request of Kinross' increasingly concerned finance department, another internal audit was conducted, reaching nearly identical conclusions. For example, at both mines, purchase orders were created after invoices were received or were not created at all. Additionally, disbursements were made without required signatures, or the signatures failed to indicate the names and positions of approval for verification purposes.

According to the SEC, Kinross management once again failed to take sufficient remedial action. As a result, from 2012 to 2015, the mines made various questionable payments. For example, between 2012 and 2014, a government customs officer was paid for weeks of fixed travel expenses, although he did not travel. Also in 2012, after Kinross' mining permit was delayed, a third-party consultant's $12,000 fee was paid using petty cash for services purportedly provided a year earlier pursuant to an oral contract between Kinross and the consultant. The permit was approved a month after the payment was made. The SEC alleged that Kinross failed to fairly describe these transactions in its books and records.

In 2013, Kinross enhanced its accounting and compliance controls for procurement and payments; however, Kinross failed to maintain these controls, according to the SEC. For example, in 2014, Kinross awarded a $50 million logistical support contract to a less-qualified shipping company with ties to a Mauritanian government official, over a more technically qualified, cheaper competitor. Additionally, Kinross retained and paid $715,000 to a politically exposed consultant without conducting proper enhanced due diligence as required by Kinross's supply chain policy. The SEC also noted that Kinross did not provide adequate anti-corruption training to its senior management.

In determining the appropriate resolution, the SEC recognized Kinross' efforts to address its internal accounting and compliances failures, such as conducting additional internal audits, implementing a new ERP system, replacing personnel at both mines, expanding the compliance team, updating relevant policies, conducting compliance training, and instituting formalized procedures to track the use of petty cash. Kinross also agreed to terminate all long-standing agreements with third-party consultants to obtain visas and permits.

6. Koolman and Parker

In April 2018, Egbert Yvan Ferdinand Koolman, a Dutch citizen residing in Miami who had served until 2016 as product manager for the Aruban state-owned telecommunications provider, Servicio di Telecommunicacion di Aruba N.V. ("Setar"), pleaded guilty to one count of conspiracy to commit money laundering in connection with funds he derived through a corrupt scheme with Florida businessman Lawrence Parker. Parker previously pleaded guilty to one count of conspiracy to violate the FCPA and to commit wire fraud related payments that he made to Koolman to earn business from Setar.

According to admissions by the two men, from November 2005 to March 2015, Parker made corrupt promises and payments to Koolman in exchange for Koolman's assistance in winning and retaining Setar telecommunications contracts for five phone companies in which Parker held an interest. Parker was a U.S. citizen residing in Miami-Dade County and all five companies were organized under the laws of, and maintained their primary places of business in, Florida. The payments were made in cash to Koolman and his ex-wife and by wire from U.S. bank accounts owned by the Parker's phone companies to foreign bank accounts owned and controlled by Koolman.

In at least two instances, Parker drew a check in his own name from an account owned by one of his phone companies and paid the amount drawn in cash to Koolman. Koolman additionally drew money from a U.S.-based bank account using a bankcard in Aruba. All told, Koolman received over $1.3 million in corrupt payments from Parker and others and drove a reported $23.8 million orders to Parker's companies.

During the relevant period, Koolman's responsibilities included interacting with vendors and purchasing mobile phones and other mobile equipment for Setar. In this position, Koolman was able to favor Parker's companies for lucrative mobile phone and accessories contracts. In addition, Koolman was able to provide Parker with Setar's confidential business information, including competing suppliers' bid information. The DOJ noted at least two instances in which Koolman sent emails with confidential competitor information to Parker's U.S.-based email account.

According to news reports, Koolman was exposed in 2016 when the Panama Papers revealed that Koolman had set up an anonymous offshore entity in the British Virgin Islands and used the company to open two bank accounts in Panama. Following an internal audit, Setar fired Koolman. In March 2017, Setar filed a civil complaint in the U.S. against Koolman, Parker and other entities and individuals.

In June 2018, Koolman was sentenced in the U.S. District Court for the Southern District of Florida to 36 months in prison and was required to pay over $1.3 million in restitution. Koolman will additionally be required to surrender himself to U.S. immigration authorities for removal following his term of imprisonment.

In April 2018, Parker was sentenced in the Southern District of Florida to 35 months in prison and was ordered to pay $701,750 in restitution. U.S. prosecutors recommended a 33% downward departure from the Sentencing Guidelines range for Mr. Parker on the basis of his substantial assistance in the prosecution of other members of the Setar conspiracy, including Koolman.

7. Panasonic

On April 30, 2018, Panasonic Corporation ("Panasonic") agreed to disgorge $126.9 million in profits and to pay $16.2 million in prejudgment interest to resolve charges with the SEC that it violated the anti-bribery, books and records, and internal controls provisions of the FCPA as well as other provisions of the Securities Exchange Act of 1934. Panasonic is a multinational electronics corporation headquartered in Japan. Its shares were traded on the New York Stock Exchange as ADRs until April 22, 2013. As a result, Panasonic was an "issuer" within the meaning of the FCPA until that time.

On the same day, Panasonic's wholly-owned subsidiary, Panasonic Avionics Corporation ("PAC"), entered into a deferred prosecution agreement with the DOJ and agreed to pay $137.4 million in criminal penalties to resolves charges that it violated the accounting provisions of the FCPA. PAC was also required to retain an independent corporate compliance monitor for a two-year term. PAC is a wholly-owned subsidiary of Panasonic. PAC designs in-flight entertainment systems and global communication systems for airlines and airplane manufacturers. PAC is headquartered in California and was therefore, at all times, a "domestic concern" under the FCPA.

In total, Panasonic and PAC paid over $280 million as a result of the misconduct described below.

a. Relevant Conduct

From 2007 to 2013, PAC used pass-through entities to make improper payments to third parties that maintained influence over contract's for which PAC was bidding. The funds for these payments originated in the Office of the President Budget, an account over which a single PAC senior executive had sole control and which was subject to very little financial oversight. Despite a 2010 internal audit report circulated to PAC executives stating the risks and potential FCPA violations associated with these practices, payments continued for several more years without interference.

According to the SEC, beginning in 1986, PAC engaged a sales representative ("Sales Representative") in the Middle East to assist with sales and contract negotiations of its products in the region. Despite having no background in avionics and warning from PAC employees on the ground that Sales Representative was paying bribes to win business for PAC, Sales Representative received more than $184 million in commissions from PAC between 2007 and 2016 through his British Virgin Islands-based corporate entity. During this time, Sales Representative presented himself as a direct employee of PAC, using PAC-branded business cards that listed him as PAC's General Manager of Sales and Marketing in the Middle East, Africa, and South Asia; maintaining an office in PAC's Dubai office; and conducting business through a PAC phone number and email address.

In 2004, PAC and a state-owned airline in the Middle East signed a Master Product Supply Agreement ("MPSA") valid for ten years. The airline appointed an executive ("Foreign Official") to serve as the primary point of contact for negotiations with PAC, and in 2006, PAC and Foreign Official began negotiations on an Amendment to the MPSA ("Amendment One"). According to the SEC, during the course of these negotiations, Foreign Official sought and obtained assistance from Sales Representative in obtaining clients for a private consulting business he had recently started.

In 2007, PAC and Foreign Official began negotiating a second amendment to the MPSA ("Amendment Two"). At the same time, Foreign Official began to solicit a high-paying position with PAC from Sales Representative. According to the SEC, as discussions regarding Foreign Official's eventual employment with PAC progressed, Foreign Official provided PAC with confidential information, advice on negotiating additional business with the Middle East airline, and tips for maintaining the relationship with airline. In September 2007, PAC offered Foreign Official a position as a PAC Consultant with annual remuneration of $200,000 plus travel expenses. Amendment Two was signed in November 2007, and, in February 2008, Foreign Official resigned from his position at the airline and was retained as a consultant by PAC. PAC disguised its consultancy relationship with Foreign Official by arranging for a separate third party to formally retain Foreign Official as a consultant and to pass through payments to Foreign Official. In this manner, Foreign Official was paid $875,000 between 2008 and 2014 from the Office of the President Budget in exchange for no demonstrable services. These payments to Foreign Official were falsely recorded in PAC's books as consulting expenses and later improperly recorded as "selling and general administrative expenses" in Panasonic's books. Between April 2007 and March 2012, PAC earned $92.8 million in profits from the Middle East airline through programs that Foreign Official had some involvement with or influence over.

Similarly, in October 2007, PAC retained as a consultant a former PAC employee who had also been hired as a consultant by one of PAC's largest domestic customers. From October 2007 to December 2013, the consultant was retained by both PAC and the customer. During this time, the consultant repeatedly provided confidential, non-public business information to PAC and used his ability and influence with the customer. Beyond providing inside and confidential information to PAC, the consultant provided few services to PAC. PAC paid the consultant a total of $825,000 from October 2007 to December 2013. PAC employees disguised payments to the consultant by using a third party as a pass-through. Compensation was improperly recorded as "consultant payments" without sufficient documentation to substantiate the nature of the payments and were ultimately improperly recorded as "selling and general administrative expenses" on Panasonic's books. PAC earned approximately $22.6 million in profits from programs that the consultant had influence over in his role as an employee for the customer.

In 2009, PAC implemented a formal review process for new and existing sales agents. The procedure required PAC employees to collect basic information regarding sales agents and for each sales agent to obtain a certification from TRACE International, a third-party non-profit organization that conducts due diligence reviews, prior to engagement by PAC. An Internal Review Committee ("IRC") then reviewed and provided final approval for each proposed sales agent. However, PAC employees subverted this process by engaging sales agents that had failed to sign the anti-bribery certification. They engaged these sales agents as sub-contractors of a certified sales agent. Between 2008 and April 2013, PAC employees directed more than $7 million to 13 uncertified sub-agents disguised as commission payments to a single certified Malaysian sales agent who then passed on payment to the sub-agents for a 1-2% fee.

The SEC noted that the implemented due diligence procedures were ineffective. The SEC stated that the IRC never rejected a proposed sales agent and made judgments based only on a single-page form containing cursory information regarding proposed sales agents, not any of the due diligence documentation. Furthermore, the IRC did not question the decline in the number of agents used after due diligence requirements were implemented, nor did it take issue with the ability of one Malaysian sales

agent to perform work on approximately fifty sales campaigns with twenty airlines. Likewise, PAC compliance personnel did not possess sufficient qualifications or training and failed to respond to clear red flags such as a referral by the state-owned airline customer. As a result, the SEC found that Panasonic failed to devise and maintain a sufficient system of internal controls in connection with the retention of sales agents.

In 2010, a senior finance executive at PAC requested that PAC's Internal Audit Department conduct an audit of the company's vendor selection, payment processing, and contract execution. The resulting audit report identified numerous compliance risks stemming from PAC's use of a particular third party to retain and pay consultants. Although the audit report was circulated among PAC executives in various forms from September 2010 through November 2012, PAC took no significant actions to address the issues raised and the suspect payments continued during this period.

b. Penalty

PAC did not receive voluntary disclosure credit because it did not voluntarily disclose the activity even after learning of and investigating the allegations as the result of a whistleblower complaint and civil suit. PAC's disclosure came only after the SEC requested documents from Panasonic related to potential violations of anti-corruption law. However, the DOJ did recommend that PAC receive a twenty percent discount from the low end of the U.S. Sentencing Guidelines fine range for cooperating with the DOJ's investigation. This cooperation included conducting a thorough internal investigation; making factual presentations to the DOJ; sharing facts learned during witness interviews conducted by the company; voluntarily making foreign and U.S. employees available for interview by the DOJ and SEC; alerting the DOJ to material information; collecting, analyzing, and organizing large quantities of evidence from multiple jurisdictions; and disclosing its Middle East misconduct to the DOJ when the government was not previously aware of it. PAC also received credit for significant remedial measures, including terminating several senior executives who were involved in or aware of the misconduct.

8. PDVSA Procurement Prosecutions

On July 31, 2018, authorities arrested Jose Manuel Gonzalez Testino ("Gonzalez"), a dual U.S.-Venezuelan citizen, on charges of violating and conspiracy to violate the FCPA for his role in a long-running bribery scheme to influence procurement processes at Petróleos de Venezuela S.A. ("PDVSA"), Venezuela's state-owned and state-controlled energy company. Gonzalez was only the latest individual charged in a string of enforcement actions brought against alleged participants in the PDVSA scheme. The DOJ unveiled charges against five individuals in February 2018 and one additional individual in April 2018. In total, the DOJ has announced enforcement actions against 17 individuals in connection with its ongoing effort to prosecute the perpetrators of corruption at PDVSA. Twelve of those individuals have pleaded guilty to various charges related to the FCPA and are awaiting sentencing. The government has issued forfeiture orders totaling in excess of $30 million against the charged individuals, some of whom are reportedly cooperating with authorities in the ongoing investigation.

a. Prior Enforcement Actions

From approximately 2009 until 2014, Roberto Enrique Rincon Fernandez ("Rincon"), Abraham Jose Shiera Bastida ("Shiera"), and their associates engaged in a coordinated effort to bribe PDVSA officials in exchange for new business and payment priority on outstanding invoices. Shiera, based in

Florida, and Rincon, based in Texas, owned multiple U.S.-headquartered energy companies that supplied equipment and services to PDVSA. In March 2016, Shiera pleaded guilty in the Southern District of Texas to one count of conspiracy violate the FCPA and to commit wire fraud, and one count of violating the FCPA. Three months later, Rincon pleaded guilty in the same jurisdiction to one count of conspiracy to violate the FCPA, one count of violating the FCPA, and one count of making a false statement on a tax return. The court imposed forfeiture orders against both individuals, requiring Shiera to surrender nearly $19 million. The forfeiture order against Rincon remains sealed. Sentencing for Rincon and Shiera is scheduled for February 21, 2019.

The DOJ also brought enforcement actions against associates and employees of Shiera and Rincon, including Moises Abraham Millan Escobar ("Millan"), Juan Jose Hernandez Comerma ("Hernandez"), and Fernando Ardila Rueda ("Ardila"). Millan, Shiera's former employee, pleaded guilty in 2016 to one count of conspiracy to violate the FCPA for his role as an agent of both Shiera's and Rincon's companies in connection with the bribery scheme. Sentencing for Millan is scheduled for February 21, 2019. In 2017, Hernandez, a former general manager and partial owner of one of Shiera's companies, and Ardila, a former sales director and partial owner of several of Shiera's companies, both pleaded guilty to one count each of violating and conspiracy to violate the FCPA in connection with their roles in the scheme. Hernandez and Ardila are scheduled to be sentenced on November 29, 2018. Another business owner, Charles Quintard Beech III ("Beech"), also pleaded guilty in 2017 to one count of conspiracy to violate the FCPA for his participation in a separate scheme to bribe PDVSA officials. Beech is scheduled to be sentenced on February 21, 2019.

The DOJ also charged former PDVSA officials involved in the scheme. In December 2015, Jose Luis Ramos Castillo ("Ramos"), Christian Javier Maldonado Barillas ("Maldonado"), and Alfonzo Eliezer Gravina Munoz ("Gravina") pleaded guilty to conspiracy to commit money laundering for accepting and attempting to conceal bribes from Rincon, Shiera, and others while they were PDVSA officials. Gravina also pleaded guilty to making false statements on a tax return. In May and July 2016, the court approved money judgments against Ramos, Maldonado, and Gravina, ordering them to forfeit nearly $11 million in cash combined, as well as real estate holdings. Ramos and Gravina are scheduled to be sentenced on February 21, 2019. Maldonado is scheduled to be sentenced on November 29, 2018. Their guilty pleas remain sealed.

b. De Leon, Cesar Rincon, Villalobos, Reiter, & Isturiz

On February 12, 2018, the DOJ announced charges against five former Venezuelan government officials for their alleged roles in the bribery scheme that also involved Rincon and Shiera. Two of the individuals (Luis Carlos de Leon-Perez and Nervis Gerardo Villalobos Cardenas) acted as conduits for the bribe payments initiated by Rincon, Shiera and others. The other three (Cesar David Rincon-Godoy ("Cesar Rincon"), Rafael Ernesto Reiter-Munoz ("Reiter"), and Alejandro Isturiz-Chiesa ("Isturiz")) were PDVSA employees during the relevant period and recipients of the bribe payments.

The 18-count indictment, dated August 23, 2017, charged De Leon and Villalobos with conspiracy to violate the FCPA, conspiracy to commit money laundering, and committing money laundering for their role in directing and disguising bribe payments from Rincon, Shiera, and others to PDVSA officials. The indictment alleged that between 2011 and 2013, Rincon and Shiera sent more than $27 million in bribe payments to a Swiss bank account controlled by De Leon and Villalobos. De Leon and Villalobos then

transferred the funds to other Swiss accounts to pay bribes to PDVSA officials, including Cesar Rincon, Reiter, and Isturiz. De Leon and Villalobos, who had previously held positions as foreign officials in Venezuela, were private citizens at the time of the alleged conduct.

In October 2017, De Leon, Villalobos, Cesar Rincon, and Reiter were arrested in Spain at the request of U.S. authorities. De Leon and Cesar Rincon were subsequently extradited to the U.S. Villalobos and Reiter remain in Spanish custody pending extradition. Isturiz's whereabouts are unknown.

On July 16, 2018, De Leon, a dual citizen of the U.S. and Venezuela, pleaded guilty to one count of conspiracy to violate the FCPA and one count of conspiracy to commit money laundering. De Leon admitted that he conspired with Villalobos, Cesar Rincon, Isturiz, and others to solicit bribes from Rincon and Shiera for PDSVA officials. In exchange, Rincon and Shiera obtained business advantages and received payment priority on outstanding invoices. De Leon further admitted that he conspired to launder and conceal the funds through various financial transactions, including wire transfers to accounts in Switzerland held in the name of individuals or entities other than De Leon and his co-conspirators.

On April 19, 2018, Cesar Rincon, former general manager of Bariven S.A. ("Bariven"), PDVSA's equipment procurement subsidiary, pleaded guilty to one count of conspiracy to commit money laundering. Cesar Rincon admitted to accepting and attempting to conceal bribes from Rincon and Shiera while he was a PDVSA official in exchange for offering payment priority and new contracts to Rincon's and Shiera's companies. The court ordered Cesar Rincon to forfeit approximately $7 million, equal to the amount of bribe payments he admitted to accepting. Cesar Rincon is scheduled to be sentenced on December 10, 2018.

c. Karina Del Carmen Nunez-Arias

On June 26, 2017, the United States District Court for the Southern District of Texas unsealed the September 30, 2016 indictment of Karina Del Carmen Nunez-Arias (Nunez), a former purchasing analyst for Bariven. The indictment charged Nunez with one count of conspiracy to violate the FCPA and to commit money laundering, accusing Nunez of accepting bribes from the owners of U.S.-based companies in exchange for favorable treatment with PDVSA. Nunez pleaded guilty in October 2016.

According to the indictment, from 2010 to 2013, Nunez, while serving as a PDVSA official, accepted bribes from Rincon and Shiera and agreed to place their companies on bidding panels for PDVSA projects. The indictment also alleged that Nunez participated in efforts to conceal the bribes by receiving payments from companies controlled by Rincon or Shiera but not in business with PDVSA, by directing payments to bank accounts registered to Nunez's relatives, and by purchasing a house in Florida with the proceeds of the bribery. Nunez pleaded guilty on October 17, 2016, although her plea remains sealed. The court ordered Nunez to forfeit the proceeds of the sale of the Florida house purchased with bribery proceeds, totaling nearly $900,000. Nunez is scheduled to be sentenced on November 26, 2018.

d. Juan Carlos Castillo Rincon

On April 11, 2018, Juan Carlos Castillo Rincon ("Castillo") was indicated on one count of conspiracy to violate the FCPA, three counts of violating and aiding and abetting violations of the FCPA,

and one count of conspiracy to commit money laundering. Castillo, a naturalized U.S. citizen and resident of Texas, managed a Texas-based company that performed logistics services for PDVSA. According to the indictment, from 2011 until at least 2013, Castillo gained improper advantages from PDVSA Services, Inc., PDVSA's wholly owned U.S.-based purchasing subsidiary, by paying bribes to PDVSA officials. Some of the payments, which occurred in the U.S. or involved U.S. bank accounts, were specifically intended to induce the official to help Castillo's company win contracts, provide Castillo with insider information, or request advantageous modifications of existing contracts between Castillo's company and PDVSA. The indictment further alleges that Castillo attempted to conceal those payments by submitting fraudulent invoices for services never performed. Castillo's trial is scheduled for October 2018.

e. Jose Manuel Gonzalez-Testino

As noted above, authorities arrested Gonzalez on July 31, 2018 for violating and conspiracy to violate the FCPA. According to an affidavit in support of the criminal complaint, Gonzalez, a dual U.S.-Venezuelan citizen, controlled multiple energy companies based in the U.S. and Panama that supplied products and services to PDVSA. The affidavit alleges that Gonzalez and others conspired to bribe PDVSA officials in exchange for receiving favorable treatment for Gonzalez's companies. Specifically, the government alleges that Gonzalez paid at least $629,000 to a former PDVSA official in exchange for new contracts, payment priority, and favorable contract terms such as payment in U.S. dollars instead of Venezuelan bolivars. The affidavit further states that two former PDSVA officials, including the one that Gonzalez allegedly bribed, have already pleaded guilty in connection with the PDVSA bribery scheme and are cooperating with authorities. Gonzalez remains in detention while his case is pending.

9. Petrobras

On September 27, 2018, Petrobras reached simultaneous agreements with authorities in the United States and Brazil in relation to a series of massive bribery and bid-rigging schemes overseen by Petrobras executives and others over the course of nearly a decade. In the U.S., Petrobras entered into a Non-Prosecution Agreement (the "NPA") with the DOJ and a settlement with the SEC, which resulted in a cease and desist order ("Order"). In Brazil, Petrobras entered an agreement to reach a settlement with Brazil's Federal Prosecution Service, the Ministério Público Federal ("MPF"). At all relevant times, Petrobras's common and preferred stock was registered with the SEC pursuant to Section 12(b) of the Exchange Act and traded on, inter alia, the New York Stock Exchange as American Depositary Shares ("ADSs"), making Petrobras a U.S. issuer for the purposes of FCPA jurisdiction.

According to the charging documents, from at least 2003 to 2012, senior Petrobras executives colluded with Petrobras's largest contractors and suppliers to intentionally inflate the cost of Petrobras's ongoing infrastructure projects by billions of dollars. The Petrobras executives took kickbacks in the range of 1-3% from these inflated contracts. Executives then passed along a portion of this money to the Brazilian politicians who had helped install the executives in their roles at Petrobras. For example, in 2005, Petrobras announced its intention to complete the construction of the Abreu e Lima Refinery ("RNEST") in Brazil. Certain Petrobras executives worked together to ensure that certain contractors were invited to bid for the various contracts involved in the RNEST construction. One executive shared with the cartel of bidders the final list of contractors that would be invited to facilitate coordination among the bidders to rig the process. According to the SEC, in exchange for the information and the structuring,

the winning contractor paid hundreds of millions of dollars to the Petrobras officials and certain politicians and political parties.

Per the SEC Order and NPA, Petrobras did not have in place a system of internal controls sufficient to provide reasonable assurances that SEC and other filings were accurate and, in fact, the SEC noted a number of material misstatements and omissions in Petrobras's financial statements and Forms 20-F from 2009 – 2013. For example, Petrobras included the kickbacks from the corruption scheme in the carrying amount of the company's property, plant, and equipment ("PP&E") in the company's 20-F forms filed starting in May 2010 and through 2014. In its Form 6-K for the quarter ending September 30, 2014, Petrobras ultimately wrote off nearly $2.6 billion of capitalized costs, representing the estimated overpayment amounts attributable to the kickbacks included in the inflated PP&E. The SEC noted a number of other misstatements, including with regard to the qualifications of its executives who, the SEC noted, were not chosen by virtue of their knowledge or specialization, but rather due to their roles in a corrupt patronage system. Certain executives were found to have knowingly and willfully failed to implement a sufficient system of internal controls to facilitate the payment of illegal bribes.

The SEC Order and NPA detail not just a single corrupt scheme, but a widespread practice of corruption among senior Petrobras executives. In one illustrative example included in the SEC Order, a Petrobras executive directed the purchase of a Texas oil refinery from a Belgium company in 2006, despite the fact that the executive was aware that the refinery had deteriorated and that its oil did not meet Petrobras's needs. In return for directing the purchase, the executive received a $2.5 million bribe.

Petrobras consented to the entry of the SEC Order, which asserted claims against Petrobras for violations of the books and records and internal controls provisions of the FCPA as well as violations of Sections 17(a)(2) and 17(a)(3) of the Securities Act and Section 13(a) the Exchange Act. In accepting Petrobras's offer of settlement, the SEC noted Petrobras's "significant" cooperation, including the fact that Petrobras has served as "Assistant to the Prosecution" in 51 proceedings in Brazil. The SEC also noted various critical remedial measures taken by Petrobras, including enhancing the compliance function, creating a Division of Governance and Compliance, enhancing controls around procurement and due diligence of contractors, and replacing the entire Board of Directors and Executive Board.

Under the terms of the NPA, Petrobras accepted its responsibility under U.S. law for the books and records and internal controls violations of its officers, directors, employees, and agents. Petrobras also committed to, among other actions, continue to improve its compliance program and trainings, conduct periodic risk-based reviews, and report at least annually to the DOJ during the three-year term of the NPA.

Petrobras agreed to pay a total penalty of $853.2 million. The total penalty reflected a 25% reduction off the bottom of the U.S. Sentencing Guidelines fine range. The reduction was granted to Petrobras on the basis of its cooperation with U.S. and Brazilian authorities and its remediation efforts, including its completion of a "thorough and timely" internal investigation, replacement of its Board of Directors and Executive Board, and introduction of an enhanced compliance program. Under the terms of the various agreements, the total penalty was divided, with Petrobras agreeing to pay $85.32 million (10%) each to the DOJ and SEC and $682.56 million (80% of the total penalty) to Brazilian authorities. The Brazilian payment does not include an attribution of liability and will be allocated to social and educational programs to promote integrity and transparency in the public sector in Brazil.

In addition to the $853 million penalty, Petrobras agreed to pay a total of $933 million in disgorgement and prejudgment interest to the SEC. Per the SEC order, any payments made by Petrobras to the class action settlement fund created in the matter of *In re Petrobras Securities Litigation*, No. 14-cv-9662 (S.D.N.Y.) were to be credited against the required disgorgement and prejudgment interest payments. The class action settlement had been granted final approval in June 2018, with Petrobras agreeing to pay $2.95 billion to settle the lawsuit. The judge awarded a total of $186.5 million in attorneys' fees in the case. The class action settlement did not include an admission of guilt. In a securities filing released alongside the SEC and DOJ agreements, Petrobras noted that the SEC would credit payments Petrobras had already made in relation to the class action, and confirmed that Petrobras would not make any additional payments to the SEC, beyond the $85.32 million penalty.

10. Eberhard Reichert—Siemens

On March 15, 2018, seven years after he was first indicted, Eberhard Reichert, the former Executive Director for Foreign Data Processing at Siemens Business Services GmbH & Co. OGH ("SBS"), a subsidiary of Siemens Aktiengesellschaft ("Siemens"), pleaded guilty to one count of conspiracy to violate the FCPA's anti-bribery provisions, accounting provisions, and wire fraud. Reichert, along with seven co-conspirators, were first charged in 2011 in connection with a decades-long scheme to bribe Argentinian officials in connection with a national identity card project valued at approximately $1 billion.

As discussed in-depth in the analysis of Siemens' 2008 settlement (*see* Hughes Hubbard FCPA & Anti-Bribery Compendium, "Siemens"), Siemens and its subsidiary in Argentina paid over $100 million to current and former Argentine government officials between 1996 and 2009 as part of its campaign to win and maintain the identity card project. Many of these payments were made through a consulting group that funneled money to high-level Argentine officials who could influence the project. Other payments were made to entities controlled by members of the Argentine government and to other entities that acted as conduits for bribes.

In December 2011, the DOJ indicated eight former Siemens executives and agents, alleging that they participated in the bribery scheme in Argentina. According to the indictment, Reichert worked for Siemens from 1964 until about 2001. Among other things, Reichert was involved in the scheme to pay millions of dollars to entities that purportedly provided services for Siemens, but which merely served as conduits for bribe payments to various Argentinian officials and politicians. Reichert participated in meetings in which these illicit payments were planned, and also signed contracts with the conduit entities. Reichert was also involved in a transaction in which a fake foreign currency hedging transaction was used to conceal improper payments to Argentinian officials.

Reichert was arrested in Croatia in September 2017 and voluntarily agreed to be extradited to the United States in December 2017. In March 2018, he pleaded guilty to one count of conspiracy to violate the FCPA and commit wire fraud, and is currently awaiting sentencing. Reichert is only the second of the eight defendants to face U.S. charges. In 2015, Andres Truppel, the former CFO for Siemens Argentina, pleaded guilty to the same charge of conspiracy to violate the FCPA and commit wire fraud. Tuppel is also still awaiting sentencing. The six remaining defendants are all still at large.

11. Sanofi

On September 4, 2018, the SEC accepted an offer of settlement from the French pharmaceutical giant Sanofi, resolving claims that Sanofi violated the FCPA's internal accounting controls and recordkeeping provisions. The SEC alleged that Sanofi subsidiaries organized in Kazakhstan, Lebanon, and the United Arab Emirates (UAE) made and kept false records of improper payments to healthcare professionals in exchange for the distribution of Sanofi products. The accounts and records of these subsidiaries were rolled up into Sanofi's books and records. Sanofi agreed to pay disgorgement in the amount of $17.6 million, prejudgment interest of $2.7 million, and a civil penalty of $5 million.

The SEC alleged that from 2007 to 2011, employees of Sanofi's Kazakh subsidiary engaged in a scheme to bribe Kazakh officials, with the assistance of local distributors, in order to influence the award of public tenders to Sanofi. The multistage process involved conspiring with distributors to inflate the sales price of products to fulfill public tenders and using the difference between the public sales price and the price Sanofi charged the distributors (typically a 20-30% difference) to create a slush fund from which bribes could be paid. Once Sanofi and the distributor agreed on an amount to be paid as a bribe, the distributor would return that amount to Sanofi employees (out of the created slush fund) to deliver to the Kazakh officials. These payments were referred to in internal records as "marzipans." According to the SEC, Sanofi earned approximately $11.5 million in profit using this scheme.

Employees of Sanofi's Lebanese subsidiary allegedly engaged in various schemes between 2011 and 2013 to increase Sanofi product sales through prescriptions. As one example, the SEC described a request by a healthcare professional at a large hospital in Jordan for several samples of an expensive cancer drug. This individual was a member of the hospital's tender committee. Although Sanofi's corporate policy required a medical justification for the cancer drug's distribution, the SEC alleged that no such justification was recorded in reviewing or approving the distribution of these drugs to the healthcare professional. Sanofi's subsidiary provided the healthcare professional 24 vials of the drug as "samples," equal to nearly 20% of the hospital's purchases of the drug. The SEC alleged that Sanofi also paid this individual over $160,000 in undocumented consulting, speaking, and clinical trial fees. Through this and other similar schemes in the region, Sanofi alleged derived profits of approximately $4.2 million.

From 2012 to 2015, sales managers and medical representatives in Sanofi's Gulf operations allegedly perpetuated a scheme to submit false travel and entertainment expenses and use the unwarranted reimbursement in order to corruptly compensate local healthcare professionals for increasing prescriptions of Sanofi products. As part of the scheme, medical representatives were instructed by local sales managers to submit false reports and doctored receipts for round table meetings with doctors that never occurred. The sales managers approved the reimbursement of costs related to these fabricated events and the proceeds were used to create a slush fund from which to make corrupt payments to health care professionals to increase prescriptions of Sanofi products. According to the SEC, Sanofi earned profits of approximately $1.75 million through this scheme.

All told, Sanofi's alleged violations resulted in profits of over $17 million. The SEC recognized Sanofi's pre-settlement remedial actions, which included providing regular briefings of its internal investigation to SEC staff, updating its internal controls and procedures governing interactions with local healthcare professionals, posting compliance personnel in high-risk local markets, terminating or disciplining over 160 employees, and accepting the resignation of 14 other employees.

In addition to its agreement to pay approximately $25 million to resolve these claims, Sanofi agreed to make three reports to the SEC over a two-year time period detailing its remedial efforts, submit any external audit reports generated during the two-year period, and cooperate with the SEC's investigations and other proceedings arising out of the allegations set forth in the settlement.

12. Société Générale and Legg Mason

On June 4, 2018, Société Générale S.A. ("Société Générale"), a global financial institution headquartered in Paris, France, and its wholly-owned subsidiary, SGA Société Générale Acceptance N.V. ("SGA"), agreed to pay a total of $585 million to U.S. and French authorities in order to resolve a coordinated investigation into a multi-year scheme to bribe Libyan foreign officials. With the DOJ, Société Générale entered into a three-year deferred prosecution agreement ("DPA") and agreed to pay a total criminal penalty of $585 million to resolve one count of conspiracy to violate the anti-bribery provisions of the FCPA. The DPA also settled a second count relating to the Société Générale's attempted manipulation of and false reporting in connection with London Interbank Offered Rate (LIBOR) for the U.S. Dollar and Yen.

SGA pleaded guilty in the Eastern District of New York ("EDNY") to one count of conspiracy to violate the anti-bribery provisions of the FCPA and was fined $500,000 (credited against Société Générale's total criminal penalty).

Société Générale also reached a settlement with Parquet National Financier (PNF) in Paris related to the same conduct, agreeing to pay approximately $293 million. The DOJ credited the amount agreed to be paid by Société Générale to the PNF against the total criminal penalty agreed in the DPA.

On the same day, Société Générale's co-conspirator, Maryland-based investment management firm, Legg Mason Inc. ("Legg Mason") and its subsidiary, Permal Group Ltd. (Permal), agreed to pay $64.2 million in criminal penalties and enter into a non-prosecution agreement ("NPA") to settle charges with the DOJ related to the same scheme. Three months later, on August 27, 2018, the SEC issued a cease-and-desist order against Legg Mason for books and records and internal controls violations of the FCPA for the same underlying conduct. Under the SEC order, Legg Mason agreed to $28 million in disgorgement and $7 million in prejudgment interest.

a. The Bribery Scheme

After the easing of economic sanctions against Libya in 2004, the Libyan sovereign wealth fund (Libyan Investment Authority ("LIA")) and other Libyan state institutions sought to invest substantial funds with international financial institutions. To secure investments, Permal and Société Générale conspired to funnel bribes to multiple Libyan officials through a Libyan-Italian agent ("Agent"). The Agent was "the right arm" and the "enforcer" of a close relative (and a bribe payment recipient) of then-Libyan dictator Muammar Gaddafi.

In total, between 2005 and 2009, Société Générale and Legg Mason paid approximately $91 million in bribes to the Agent for "introduction" services, passed through the Agent's company incorporated in Panama. Portions of these payments were then passed on to high-level Libyan officials to secure 13 investments and one restructuring, valued at $3.66 billion. Société Générale earned profits of

approximately $523 million from these deals. Seven of the 13 investment notes Société Générale sold to the Libyan state institutions (valued at $950 million) were linked in whole, or in part, to Permal. In connection with these seven transactions, Permal earned net revenues of approximately $31.6 million.

By at least 2006, two Permal employees and several Société Générale employees knew that the Agent was paying money and providing other improper benefits to Libyan government officials in order to secure lucrative investments and exclude competitors for the benefit of Permal and Société Générale. Despite that knowledge, these employees agreed to continue to use the Agent who, through the use of bribes or coercion, exerted influence over (or "cooked") relevant Libyan officials.

Permal and Société Générale also deployed measures to conceal the bribery scheme. In addition to using coded terms such as "cooked," in 2006, Permal and Société Générale conspired to hide the Agent's existence by replacing the Agent's name in relevant documents with Permal's name, and then using Permal to pass the payments to the Agent. Later, Permal and Société Générale, with the help of the Agent, conspired to persuade the LIA to amend its agent disclosure requirement to be "forward looking only," so that the past relationship with the Agent could be concealed.

Around November 2009, compliance personnel at Société Générale Corporate and Investment Bank ("SG CIB"), a division of Société Générale that offered investment banking services, indicated to their senior managers that the commissions paid to the Agent appeared unjustifiable in relation to the service rendered, based on the amounts paid and the percentage to the investment deals. The compliance personnel also raised concerns that the Agent was paid through a Panamanian company, incorporated in a country that is on the OECD's blacklist. Despite these alarms, Société Générale continued to seek to engage the Agent in a variety of capacities, including as a joint venture partner.

In mid-2010, LIA's new management made inquiries to Société Générale employees about the role of the Panamanian entity on various prior deals and the entity's owner. Following these inquiries, Société Générale's employees provided false and misleading information to LIA, including falsely stating that the remuneration paid to the Panamanian company did not affect the profitability of LIA's investments and that the company complied with all of Société Générale's internal procedures. Société Générale also failed to respond to certain inquiries and minimized disclosures in term sheets by using small font and non-standard typefaces.

b. Terms of the Resolutions

Société Générale's total criminal penalty reflects a 20% discount off of the low end of the calculated U.S. Sentencing Guidelines fine range. According to the DPA, the discount was attributed to Société Générale's efforts to conduct a thorough and robust internal investigation, collect and produce voluminous evidence located in other countries, and provide frequent and regular updates to authorities as to the status of and facts learned. Because the DOJ had developed significant independent evidence of misconduct without Société Générale's assistance, Société Générale did not receive the full 25% reduction for which it was eligible. The DOJ agreed that an independent compliance monitor was unnecessary because of Société Générale's remediation and the advanced state of its compliance program.

In addition to the DPA with the DOJ, Société Générale settled a civil dispute with the LIA and made a payment of approximately $1.1 billion to the LIA relating to the allegations of corruption.

Legg Mason's criminal penalty represented a 25% discount off of the low end of the calculated U.S. Sentencing Guidelines range, attributed to Legg Mason's substantial cooperation and remediation. In reaching the NPA, the DOJ acknowledged several mitigating factors, including: (i) the misconduct only involved two mid-to-lower level employees of Permal, a Legg Mason subsidiary; (ii) relevant employees had been disassociated with Permal for more than four years at the time of the NPA; (iii) the misconduct was not pervasive throughout the company; (iv) it was Société Générale, the co-conspirator, not Legg Mason itself, that maintained the relationship with the Agent and was responsible for originating and leading the scheme; (v) the profits earned by Legg Mason from the misconduct were less than one-tenth of the profits earned by Société Générale; and (vi) Legg Mason has no history of similar misconduct.

In declining to impose a civil penalty, the SEC also recognized Legg Mason's significant cooperation in collecting information that might not have been otherwise available to the SEC. This cooperation included summarizing the findings of its internal investigation, making employees available to the SEC (including arranging for foreign employees' travel to the United States for interviews), and providing timely factual summaries of witness interviews and other information developed in the course of its internal investigation. The SEC also considered Legg Mason's remedial action, including disciplining the employees involved in the violation, expanding the compliance function, and enhancing its internal accounting controls to prevent and detect the type of similar misconduct in the future.

13. Stryker

On September 28, 2018, Stryker Corporation agreed to settle charges with the SEC that it had violated the FCPA's books and records and internal accounting controls provisions through its operations in China, India, and Kuwait. As part of the resolution, without admitting or denying the allegations, Stryker agreed to pay a $7.8 million civil penalty and to appoint an independent compliance consultant for a period of 18 months to review and evaluate Stryker's ethics and compliance function, internal controls, record-keeping, and anti-corruption policies and procedures, especially regarding third parties such as dealers, agents, distributors, and sub-distributors. The independent compliance consultant will issue a written report within six months of being retained, after which Stryker will have 90 days to implement any recommendations. After 180 days, the Compliance Consultant will perform a follow-up review.

Stryker had previously paid $13.2 million to settle charges with the SEC in October 2013 that it had violated the FCPA's books and records and internal accounting controls provisions with regard to improper payments made to doctors and officials at government-run hospitals in Argentina, Greece, Poland, and Romania. The SEC alleged that Stryker had falsely recorded these expenses as charitable donations, consultant fees, travel expenses, and commission payments.

Stryker is a Michigan-based producer of medical technologies including implants, surgical equipment, medical devices, and emergency medical equipment. At all relevant times its shares were registered with the SEC under section 12(b) of the Exchange Act and were traded on the New York Stock Exchange, making it an "issuer" under the FCPA.

a. Misconduct in China, India, and Kuwait

In India, Stryker's wholly-owned subsidiary Stryker India generated 85% of its sales revenue through sales to third-party dealers. Stryker's global compliance and accounting policies and procedures applied to each dealer, including a prohibition on improper payments to government or non-government officials, employees, or entities and a requirement for each dealer to maintain complete and accurate records regarding their distribution of Stryker products. According to the SEC, in 2012, Stryker India received allegations of misconduct by its dealers and investigated three, finding inadequate record-keeping and internal accounting controls at all three. One dealer was terminated and certain corrective actions were implemented regarding the remaining two dealers investigated. However, despite numerous red flags and complaints, the SEC alleges that Stryker India failed to perform an audit of the rest of its third-party dealers until 2015. According to the SEC, the 2015 audit revealed that Stryker India's inadequate controls had allowed its dealers to submit inflated invoices to hospitals at their request so that the hospitals could pass along the falsely inflated charges to patients and their insurance carriers. The SEC further alleges that Stryker India failed to maintain accurate books and records and repeatedly authorized payments to third parties without documentation to establish a legitimate business purpose. Upon examination of a sample of Stryker India's highest-risk transactions, the SEC found that over 27% had no accompanying documentation whatsoever.

In China, Stryker's wholly-owned subsidiary, Stryker China, sold products through a state-owned "hub"-distributor that, in turn, re-sold products through a network of sub-distributors. According to the SEC, between 2015 and 2017 at least 21 sub-distributors sold Stryker's products in China without going through any type of review, approval, or training by Stryker China. The SEC alleged that, in some cases, third, fourth, and fifth tier sub-distributors were even engaged to sell Stryker's products, all without approval or training and in violation of Stryker's accounting controls policies. Furthermore, the SEC alleged that in certain cases Stryker China employees worked directly with the unauthorized sub-distributors and, in other cases, purposefully concealed the involvement of the sub-distributors. According to the SEC, Stryker's deficient internal accounting controls failed to detect or prevent the use of unauthorized and untrained sub-distributors, increasing the risk that Stryker funds could have been used to pay bribes or fund other types of misconduct.

In Kuwait**,** employees of Stryker's Netherlands-based wholly-owned subsidiary oversaw sales of Stryker products to the Kuwait Ministry of Health through one primary distributor. From 2015 to 2017, Stryker allegedly held a number of events for Kuwaiti healthcare providers where Stryker paid for meals, accommodations, and local travel directly. However, according to the SEC, Stryker's Kuwaiti distributor paid $32,000 in additional "per diems" related to these events that were not detected by Stryker's internal accounting controls. According to the SEC, when Stryker tried to exercise its audit rights, the distributor refused. As a result, the SEC alleged that Stryker's internal accounting controls had failed to test or otherwise assess whether the distributor was complying with Stryker's anti-corruption policies.

b. Remediation

The SEC considered Stryker's cooperation and remedial efforts in reaching the settlement. In terms of cooperation, the SEC pointed to the facts that Stryker hired counsel to conduct an internal investigation into its operations in India, China, and Kuwait and shared its findings with the SEC on an ongoing, voluntary basis in cooperation with the SEC's own investigation. Stryker also updated its

policies and procedures in India, introduced additional controls around its monitoring of dealership and distributorship relationships, created new third-party due diligence controls, increased training for all Stryker India employees, created a centralized system for documentation to increase transparency in India, conducted compliance audits of marketing events and reimbursements in India, and audited its dealers' and distributors' business practices in India. Stryker also appointed new leadership for Stryker India, terminated senior employees at Stryker India, terminated its distributor in Kuwait, and strengthened its compliance program with special attention to due diligence and documentation related to consultants and distributors.

14. Transport Logistics International and Mark Lambert

On January 1, 2018, the DOJ charged Transport Logistics International, Inc. ("TLI") with conspiracy to violate the anti-bribery provisions of the FCPA in order to obtain and retain uranium transportation contracts. Two months later, the company entered into a three-year Deferred Prosecution Agreement related to the charges. Under the DPA, TLI agreed to pay a $2 million penalty. TLI also agreed to institute an enhanced compliance program and conduct a review of its internal accounting controls. Given its size and risk profile, TLI was not required to retain an independent compliance monitor.

On January 12, 2018, the DOJ also unsealed an 11-count indictment against former TLI owner and executive Mark Lambert. Lambert faces one count of conspiracy to violate the FCPA and to commit wire fraud, seven counts of violating the FCPA, two counts of wire fraud, and one count of money laundering. Lambert is only the latest individual prosecuted in connection with the scheme; the DOJ secured guilty pleas from three other individuals in 2015 for related conduct.

a. TLI

TLI is a Maryland-based transportation company that provides shipping services for nuclear materials both within the United States and abroad. The charges against TLI arose from its role in the so-called "Megatons to Megawatts" project, an agreement between the U.S. and Russia for the disposal of enriched uranium from disassembled Russian warheads by downgrading and selling it to U.S. nuclear energy providers. From 1995 until 2013, the program saw the conversion of 475 metric tons of high-grade uranium—the equivalent of 19,000 warheads—into low-grade uranium, which was then sold in the U.S. JSC Techsnabexport ("TENEX"), a subsidiary of Russia's State Atomic Energy Corporation ("ROSATOM"), was responsible for the sale and transportation of this vast quantity of material to the U.S. TENEX selected TLI as one of its transportation providers.

According to admissions by TLI, from 2004 to 2014, TLI and certain individuals conspired to pay approximately $1.7 million in bribes to Russian national Vadim Mikerin (at the time a Director of TENEX) to secure improper advantages in gaining and retaining business with TENEX. The co-conspirators discussed the bribes in coded language and created false invoices to disguise TLI's illicit payments. In one example, then-TLI owner and executive Daren Condrey instructed a TLI employee to create an invoice for $8,157 to "get commissions off the books." TLI then paid that amount to a bank in Cyprus based on the fraudulent invoice. The following day, another co-conspirator wrote Mikerin to confirm the payment, stating that "Cake was delivered yesterday as planned." Mikerin used similar language to request bribes, asking, for example, that a certain co-conspirator "please confirm [his] ability to support

TLI's Cake Cooking on a regular basis once per [quarter] at 5% net volume." In exchange for these kickbacks, Mikerin ensured that TENEX would continue to award contracts to TLI.

In determining the appropriate fine for TLI's misconduct, the DOJ noted TLI's failure to voluntarily and timely disclose its conduct and thus declined to provide any voluntary disclosure credit. The DOJ did, however, provide TLI with full credit for its substantial cooperation in the investigation. Specifically, TLI earned credit for reviewing emails and financial statements, voluntarily producing pertinent documents, and providing interviews with relevant witnesses, including one Russian witness who was otherwise inaccessible to prosecutors. TLI also provided information about the other individuals involved in the misconduct and engaged in remedial measures up to and including termination of all individuals who participated in the scheme. The DOJ granted TLI a 25% reduction off the lower end of the sentencing range for its cooperation and remediation and determined the appropriate penalty was $21,375,000. The 25% reduction is the maximum allowable for a company that does not voluntarily disclose misconduct per the DOJ's FCPA Corporate Enforcement Policy.

However, TLI represented that a penalty greater than $2 million would substantially jeopardize the company's continued viability. Based on that representation, and after conducting an independent ability-to-pay analysis, the DOJ determined that that a penalty of $2 million was appropriate. The DOJ also credited approximately $220,000 in seized funds against the penalty.

b. Mark Lambert and Other Individuals

The DOJ brought charges against Mark Lambert, former owner and executive of TLI, alongside Condrey, for alleged acts that closely track the charges for which Condrey and TLI pleaded guilty. The DOJ alleges that Lambert and Condrey learned of the conspiracy in 2009 from an undisclosed TLI executive, and soon agreed to take part in it. In addition to the schemes described above—the use of code words to conceal the payment of bribes, and the fraudulent creation of invoices to effect those payments—the DOJ alleges that Lambert personally authorized many of the wire transfers TLI made to shell corporations for the ultimate benefit of Mikerin. Lambert's trial is scheduled to begin on April 30, 2019.

Several other individuals have already pleaded guilty to FCPA violations and other offenses in connection to the same bribery scheme. On June 16, 2015, the DOJ charged Condrey with conspiracy to violate the FCPA and conspiracy to commit wire fraud, and he pleaded guilty the following day. He is awaiting sentencing as of the time of this writing.

On August 31, 2015, Mikerin pleaded guilty to one count of conspiracy to commit money laundering. On December 15, 2015, Mikerin was sentenced to 48 months in prison. He was also ordered to forfeit $2,126,622.36—the amount transferred to offshore bank accounts in the course of the scheme.

On June 15, 2015, Boris Rubizhevsky pleaded guilty to conspiracy to commit money laundering for his participation in the scheme, which involved providing sham consulting services as a means to disguise payments to TENEX. He was sentenced to one year and one day in prison, followed by three years of supervised release, and was also ordered to forfeit $26,500.

15. United Technologies

On September 12, 2018, United Technologies Corporation ("UTC") agreed to pay $13.9 million to resolve allegations that it violated the anti-bribery, books and records, and internal controls provisions of the FCPA through payments by subsidiaries in UTC's elevator and aircraft engine businesses. Without admitting or denying the allegations, UTC consented to the SEC's cease and desist order ("Order") alleging that UTC subsidiaries Otis Elevator Co. ("Otis") and Pratt & Whitney ("Pratt") made improper payments and provided other improper benefits to government officials in Azerbaijan, China, Kuwait, Russia, Pakistan, South Korea, Thailand, and Indonesia.

In Azerbaijan, the SEC Order alleges that an Otis affiliate in Russia ("Otis Russia") engaged in various schemes to sell elevator equipment to Baku Liftremont, a municipal entity in Azerbaijan. In one such scheme, Otis Russia allegedly used two subcontractors to make payments to Liftremont officials. Otis Russia paid the subcontractors nearly $800,000 (roughly 44% of the total contract value) without appropriate documentation or any due diligence. The SEC alleged that documentation failed to establish that the subcontractors provided services to justify the compensation. In another scheme, Otis Russia engaged a series of intermediaries as distributors, offering equipment at one price while knowing that the intermediaries would sell the equipment to Liftremont at an inflated price and use the difference to pay bribes to Liftremont officials. No due diligence was performed on the intermediaries, and they were engaged without business justification; Otis Russia's JV partner was already authorized to sell products in Azerbaijan. Through these and other schemes, the SEC Order alleges that Otis Russia entered into ten contracts with Liftremont with a total value of $14.6 million.

In China, Pratt and a Pratt joint venture, International Aero Engines ("IAE"), allegedly engaged in various corrupt schemes to sell airplane engines to Chinese state-owned commercial airlines, including Air China Ltd. In 2006, at the direction of Pratt, IAE retained a Chinese sales agent to help increase market share. Neither Pratt nor IAE conducted due diligence on the agent, who had no experience in the airline industry (the agent had previously worked in the toll road business). According to the Order, from 2009 to 2013, IAE paid the agent approximately $55 million in commissions. The SEC alleged that a portion of these commissions were passed on to officials at Chinese state-owned airlines in return for contracts. The SEC also alleged that IAE and Pratt used improper sponsorships to curry favor with Chinese officials. For example, in 2009 and 2011, IAE and Pratt contributed $30,000 each for a golf event for senior executives of a Chinese airline. At the event, expensive gifts, such as iPads and luggage, were provided by IAE's Chinese agent to the Chinese officials.

The SEC Order also highlighted allegedly improper leisure travel provided by UTC for foreign officials in China, Kuwait, South Korea, Pakistan, Thailand, and Indonesia. According to the SEC, UTC, through Pratt and Otis, frequently used trips and entertainment to reward or influence foreign officials. Employees allegedly sometimes circumvented UTC controls by submitting expenses for travel of foreign officials without disclosing the leisure aspect of the travel. The SEC faulted the legal department and supervisors for failing to identify red flags prior to approving these expenses. For example, the SEC noted that official travel for foreign officials to Orlando was approved despite the fact that Pratt did not have a facility there (and that it is a popular tourist destination). In other instances, UTC allegedly provided improper leisure travel in conjunction with legitimate business travel. In some instances, the leisure portion of the trips was four times as long as the business portion. In total, the SEC alleged that

between 2009 and 2015, UTC recorded $134,000 in improper travel and entertainment for foreign officials as legitimate business expenses.

In accepting the offer of settlement, the SEC took into consideration that UTC self-reported the misconduct, cooperated fully with the SEC's investigation, and engaged in extensive remedial measures, including the termination of employees and third parties involved in the misconduct.

B. 2017

1. Joseph Baptiste

On October 4, 2017, the U.S. federal prosecutors charged retired U.S. Army colonel Joseph Baptiste in the District Court of Massachusetts with (i) conspiring to violate the Travel Act and anti-bribery provisions of the FCPA, (ii) violating of the Travel Act, (iii) and laundering money in connection with a scheme to pay bribes to Haitian officials. Initially, after being confronted by federal agents in December 2015, Baptiste signed a sworn declaration and entered into a plea agreement with the government in which he agreed to waive indictment and plead guilty to one charge of conspiring to violate the anti-bribery provisions of the FCPA and the Travel Act. However, Baptiste later decided not to continue with the plea agreement and, on October 23, 2017, pleaded not guilty to all three counts returned in the indictment.

The indictment alleges that between November 2014 and December 2015, Baptiste solicited bribes from FBI undercover agents who posed as prospective investors in a port development project (the "Port Project") in the Moles Saint Nicolas commercial development area of Haiti. Baptiste, a Maryland resident and practicing dentist, served as the president of the National Organization for the Advancement of Haitians, Inc. ("NOAH"), a Maryland-based, tax -exempt, non-profit entity set up to assist impoverished Haitians. Baptiste also served as a director of a Delaware company established to promote reconstruction projects in Haiti ("Delaware Company"). One of Delaware Company's goals was to promote the Port Project, which encompassed the construction of multiple cement factories, a shipping-vessel recycling station, an international transshipment station, a power plant, a petroleum depot, and tourist facilities.

According to prosecutors, in November 2014 Baptiste flew from Maryland to Massachusetts to meet with an undercover FBI agent ("FBI Agent 1") that Baptiste believed to be a potential investor in Haitian development projects. At this meeting, Baptiste allegedly discussed the "pay-to-play" system in Haiti, offered to introduce FBI Agent 1 to high-ranking Haitian officials, and described how Baptiste could make bribe payments to these officials and utilize NOAH to disguise the bribe payments. Baptiste also allegedly described two prior instances in which he had obtained licenses to operate in Haiti by making bribe payments to local officials. In November 2015, Baptiste and two associates allegedly met with FBI Agent 1 and a second undercover FBI agent ("FBI Agent 2") at a Boston-area hotel to solicit investments from the FBI Agents for the first phase of the Port Project. Baptiste allegedly informed the FBI Agents that the Port Project would cost approximately $84 million and would require bribe payments to high-level Haitian officials in order to obtain government approvals. Baptiste allegedly agreed to provide banking information for NOAH to the FBI Agents in order to facilitate bribe payments and, upon leaving the meeting, placed a call to a Haitian telephone number, which was intercepted by the FBI and identified as belonging to a high-level Haitian public official ("Haitian Official").

Several days later, Baptiste allegedly traveled to Haiti and requested $25,000 from FBI for Baptiste to use to gain Haitian Official's support. FBI Agent 2 wired the requested $25,000 to NOAH's U.S.-based checking account. In December 2015, Baptiste allegedly asked FBI Agent 2 for an additional $25,000, stating that several officials in Haiti had requested more money. Several days later, an associate of Baptiste's allegedly emailed a letter of support signed by Haitian Official to FBI Agent 2 and FBI Agent 2 wired an additional $25,000 to NOAH's checking account.

The indictment states that Baptiste ultimately spent the $50,000 transferred by undercover FBI Agents on personal expenses. Although Baptiste intended to direct future payments towards bribes related to Port Project, none of the $50,000 provided to him was paid to Haitian officials.

If convicted, Baptiste faces up to thirty years of imprisonment, up to $1 million or more in monetary penalties, forfeiture of any property which constitutes or is derived from proceeds of the Travel Act offense, and forfeiture of any property involved in or traceable to the money laundering offense. A jury trial is scheduled for December 3, 2018 in the U.S. District Court in Massachusetts.

2. Halliburton

On July 27, 2017, the SEC filed a cease-and-desist order against Halliburton Company ("Halliburton"). The SEC found that Halliburton, in its efforts to fulfill its local content requirements in Angola, violated the books and records and internal accounting controls provisions of the FCPA. Halliburton agreed to pay $14 million in disgorgement, $1.2 million in prejudgment interest, and $14 million in penalties to resolve the matter. The order also imposed a $75,000 civil penalty against Jeannot Lorenz, a former-Vice President of Halliburton who orchestrated transactions in violation of Halliburton's internal control provisions. Both Halliburton and Lorenz consented to the order without admitting or denying the SEC's findings.

The SEC also required Halliburton to retain an independent compliance consultant with FCPA expertise to review and evaluate its anti-corruption policies and procedures and report the findings to the SEC for a period of 18 months.

a. Background

Halliburton is an oilfield services company incorporated in Delaware and headquartered in Houston, Texas. At the time of the alleged FCPA violations, it employed more than 70,000 employees in over 70 countries, including Angola. According to the SEC, in 2008, Sonangol, Angola's state-owned oil production company, warned Halliburton that it may veto further subcontract work for Halliburton in Angola if it continued to fail to comply with Angola's local content regulations. Halliburton officials recognized that further partnership with local Angolan companies would be necessary to fulfill the local content obligations. Halliburton asked Jeannot Lorenz, a French citizen and U.S. resident who had served as Halliburton's interim country manager in Angola, to oversee the local content efforts.

Lorenz allegedly developed a plan for Halliburton to partner with a local Angolan company that was owned by a former Halliburton executive. The SEC described the former executive as a "friend and neighbor" of a Sonangol official who could approve the award of contracts on Sonangol's behalf.

b. Books and Records and Internal Accounting Controls Violations

The SEC's order indicates that Lorenz first sought to retain the local Angolan company as a commercial agent. Under this arrangement, Halliburton would pay the Angolan company 2% of its existing revenues in Angola. Halliburton management allegedly rejected this proposal, finding it unfeasible under Halliburton's then-new due diligence processes that included involvement of outside counsel experienced in FCPA compliance.

According to the SEC, Lorenz subsequently proposed outsourcing "real estate maintenance, travel, and ground transportation services," which were typically in-house functions, to the local Angolan company. Halliburton's procurement process involved a lengthy and competitive bidding process, governed by internal accounting controls that first required assessing the need for the services before choosing a supplier. Lorenz allegedly circumvented these internal controls by entering into an interim consulting agreement with the Angolan company while the procurement process on the real estate maintenance and ground transportation services contract was pending. Under the interim consulting agreement negotiated in July 2009, Lorenz allegedly agreed that Halliburton would pay the local Angolan company $45,000 per month as a sign of good faith. The interim consulting agreement falsely stated that the Angolan company would provide reports on local content requirements and how Halliburton could meet those requirements in the areas or travel, logistics, and real estate maintenance. In entering this agreement, Lorenz failed to obtain the review and approval of a Tender Review Committee for contracts above $10,000 in high-risk countries such as Angola.

In February 2010, Halliburton and the local Angolan company finalized the interim consulting agreement, which was backdated to September 2009. Halliburton allegedly paid the local Angolan Company $405,000 for the period between September 2009 and May 2010, but the Angolan company had not actually provided any of the services for which it was contracted. Also in February 2010, the bidding process for the real estate maintenance and ground transportation services concluded. The local Angolan company was the least successful bidder and was substantially more expensive than the next highest bids. Even so, Lorenz sought a way to grant the contract to the local Angolan company, despite the availability of other Angolan companies that could satisfy the local content requirements. His efforts were fruitless, and the local Angolan company refused to lower its bid.

Lorenz then developed another proposal whereby the local Angolan company would lease commercial and residential real estate and then sublease such real estate to Halliburton. According to the SEC, Lorenz selected the supplier before determining the critical services, contrary to Halliburton's internal accounting controls. In addition, Lorenz did not, as required by Halliburton's internal policies, consult Halliburton's Real Estate Services department to manage the process initially. According to the SEC, in May 2010, Halliburton and the Angolan company executed a Real Estate Transaction Management Agreement. The agreement called for compensation to the local Angolan company of $275,000 per month for real estate transaction management. The SEC alleged that the local company did not provide meaningful services under the agreement and failed to provide any of the required reports.

Halliburton ultimately terminated the relationship with the Angolan company in April 2011 after receiving an anonymous email in December 2010 alleging possible misconduct surrounding the transactions with the local Angolan company. Throughout the course of the interim consulting agreement and the final agreement, from April 2010 through April 2011, Halliburton paid the local Angolan company

$3,705,000 and received seven subcontracts from Sonangol that led to nearly $14 million in profit. According to the SEC, Halliburton recorded these payments as payments for services under the relevant contracts, when in fact they were made solely to fulfill Halliburton's local content requirements. The SEC found this to be a violation of the FCPA's books and records provisions.

3. Heon Cheol Chi

On July 17, 2017, Heon-Cheol Chi ("Chi"), a researcher and director at the Korea Institute of Geoscience and Mineral Resources (KIGAM), was found guilty in the U.S. District Court for the Central District of California of transacting in criminally derived property in violation of 18 U.S.C. § 1957. Chi accepted payments from seismological companies in violation of South Korea's anti-bribery statute. He funneled a portion of the funds through the U.S. banking system, giving rise to the money laundering charges. On October 2, 2017, District Judge John Walker sentenced Chi to 14 months in prison.

a. The Bribery and Money Laundering Scheme

According to the DOJ's first superseding indictment, Chi, a South Korean citizen, became a principal researcher at KIGAM in approximately 2003 and served as the Director of KIGAM's Earthquake Research Center beginning in approximately 2011. Between roughly 2009 and 2015, Chi accumulated over $1 million in payments from two seismological companies doing business with KIGAM and other South Korean customers. Press reports identified the companies that made these payments as Guralp Systems Ltd. ("Guralp"), based in the United Kingdom, and Kinemetrics, based in California. Over the course of the relevant period, Guralp paid approximately $650,000 and Kinemetrics paid approximately $386,000 toward what Chi sometimes called his "advice fee." Guralp and Kinemetrics deposited the funds in Chi's Bank of America account in California. From there, Chi moved about half the money to a brokerage account in New York and spent most of the remainder in South Korea. The DOJ's July 18, 2017 press release indicated that the funds from Guralp and Kinemetrics overshadowed Chi's legitimate salary "by a substantial margin."

In exchange for Guralp's and Kinemetrics's payments, Chi provided the companies with unfair business advantages. The DOJ's press release states that Chi supplied the companies with confidential information about the bidding process at KIGAM, shared further confidential information about the companies' competition, and directly advocated for their products and services when KIGAM and other customers were making procurement decisions.

The DOJ characterized Chi as a public official whose acceptance of bribes violated Article 129 of South Korea's Criminal Code, which prohibits officials from receiving, demanding, or agreeing to accept bribes in connection with their official duties. Prosecutors noted that KIGAM takes its funding from the government of South Korea, and also tests and certifies the government's seismological equipment.

The DOJ presented evidence that Chi knew he was a public official and that his actions violated Korean law. For example, in 2014, Chi wrote to a representative of Guralp, "I am a governmental officer and I should not have any contact with [a] private company. Moreover, it is illegal to assist any company related to the test." Ironically, Chi also left a paper trail discussing his practice of destroying evidence. In its July 18, 2017 press release, the DOJ highlighted a 2005 email from Chi to one of the companies that

bribed him, stating, "[u]sually I delete[] almost all e-mail or papers related to [the payments in question] because I am the director of earthquake research center and I am not allowed to be involved in it."

Furthermore, the DOJ also obtained emails from Chi discussing the money laundering scheme for which he was eventually convicted. In one such email to a representative of Guralp in 2010, Chi remarked that his position forbade him from "participat[ing] in private companies," explained that he was required to furnish the government with an annual income report, and ultimately told the representative, "[t]hat is why I got the advice fee from you through the American bank."

b. Sentencing and Fallout

Although Chi was charged with six counts of transacting in criminally derived property totaling $306,000, the jury returned a guilty verdict on only one count concerning a $56,000 transaction. The jury hung on the remaining five counts. Prosecutors reportedly sought a prison sentence of 57 to 71 months, emphasizing the totality of Chi's conduct. Chi's defense, on the other hand, argued that only the $56,000 transaction should be considered at sentencing and advocated for a term of just six months.

4. Patrick C.P. Ho

In November 2017, a criminal complaint ("Complaint") was unsealed charging Chi Ping Patrick Ho, a.k.a. Patrick C.P. Ho a.k.a. He Zhiping ("Ho"), and Cheikh Gadio with conspiring to violate the FCPA, violating the FCPA, conspiring to commit international money laundering, and committing international money laundering. During the relevant time period, Ho was the Deputy Chairman and Secretary-General of the China Energy Fund Committee ("CEFC"). Gadio was the Senegalese Minister of Foreign Affairs from approximately 2002 to 2009.

In December 2017, Ho was formally indicted. He is awaiting trial. In September 2018, the DOJ requested that the charges against Gadio be dismissed. At the same time, Gadio's attorneys indicated that Gadio was looking forward to continuing his cooperation with U.S. authorities.

The eight-count indictment against Ho filed in the Southern District of New York describes a major scheme to bribe officials at the highest levels of the Ugandan and Chadian governments for the benefit of CEFC, a Chinese oil and gas conglomerate. CEFC is headquartered in Shanghai, with $39 billion in revenue in 2015 and with affiliates worldwide, including in New York. CEFC funds the NGO of which Ho was the Secretary-General and Deputy Chairman. The NGO is based in both Hong Kong and the United States and held or holds Special Consultative Status with the UN Economic and Social Council. The NGO's Special Consultative Status afforded Ho access to meetings with UN officials that are not open to general members of the public.

Prosecutors are asserting jurisdiction over Ho on the basis that he was an agent of a domestic concern and that he took actions in furtherance of the scheme while in the United States.

As alleged in the Complaint, Ho and Gadio conspired to bribe African government officials, including Chadian President Idriss Deby, to secure oil rights and other business benefits for CEFC. The Complaint focused on two separate conspiracies, one targeting Chad and the other targeting Uganda. Both conspiracies are alleged to have been initiated in the halls of the United Nations while Sam Kutesa, who later became the Foreign Minister of Uganda, served as President of the General Assembly. Both

the Chad and Uganda conspiracies are alleged to have lasted from at least in or about late 2014 through January 2017.

a. Chadian Scheme

The first alleged scheme began sometime around September or October 2014. Ho allegedly sought the assistance of Gadio, who had a personal relationship with the President of Chad, and sought "special attention and support" from President Deby of Chad for CEFC. CEFC wished to enter into a joint venture with a Chinese government-owned oil and gas company, now understood to be China National Petroleum Corporation (CNPC), but that company was facing substantial legal hurdles. At the time, Chad had fined CNPC $1.2 billion for environmental violations and revoked its oil licenses. At Ho's direct request, Gadio allegedly met with the President Deby in October 2014 and conveyed Ho's offer to provide, in Gadio's words, "financial assistance for [the President's] political campaigns." In exchange, President Deby was allegedly willing to reconsider his decision to revoke CNPC's licenses. By the end of October, the government of Chad had entered into a settlement with CNPC whereby CNPC would pay $400 million, grant the government a 10% share in its active oilfields in Chad, and grant a 25% stake in future productive fields. In exchange, Chad dropped its arbitration case against CNPC.

Ho, Gadio, and Deby allegedly continued to communicate regarding CEFC's business interests, particularly with regard to various oil rights owned by CNPC. In December 2014, on the basis of Gadio's advice, Ho wrote to President Deby conveying CEFC's interest in making a $2 million "donation" to support "social and other programs" chosen by Deby. According to prosecutors, CEFC was subsequently subject to preferential treatment by the Chadian government, but was not able to successfully conclude a sought-after acquisition of Chad's 10% interest in CNPC's active oilfields. In December 2015, CEFC signed an agreement with a Taiwan's state-owned Chinese Petroleum Corp ("CPC"). The transaction closed in September 2016, with CEFC paying approximately $110 million for a 35% share of CPC's oil bocks in Chad.

b. Uganda Scheme

Shortly after Sam Kutesa began his term as President of the 69th Session of the UN General Assembly ("PGA"), Ho allegedly sought to cultivate a relationship with Kutesa with the intent to ultimately connect with the President of Uganda. Kutesa, who otherwise served as the Foreigner Minister of Uganda when not in the position of PGA, is related to the President of Uganda, Yoweri Museveni. During his time as PGA, Kutesa allegedly frequently met with Ho to discuss CEFC and the prospect of forming a "strategic partnership" between Uganda and CEFC once Kutesa returned to Uganda. In August 2015, during a trip to China, Kutesa appointed the Chairman of CEFC, Ye Jianming, as a "Special Honorary Advisor." News reports at the time indicate that Chairman Ye emphasized CEFC's interest in deepening its cooperation with Uganda, while Kutesa suggested that he would support CEFC's investment in the energy and financial sectors in Uganda and other African countries. Prosecutors allege during this trip Kutesa obtained a promise that CEFC would provide a "donation" to support Museveni's reelection campaign.

Once Museveni was reelected president and Kutesa had returned to Uganda, Kutesa allegedly solicited the $500,000 "contribution" he had previously requested. The money was described by Kutesa and others in various communications as either for the benefit of the president's reelection campaign

(which had already been concluded) or as a "donation" to "support" Kutesa. In early May 2015, Ho allegedly wired $500,000 dollars from Hong Kong through New York to a Ugandan bank account controlled by a Ugandan foundation designated by Kutesa. Prosecutors allege that during their own investigation, they could find no such organization in Uganda, and people associated with the building listed as the foundation's HQ stated that no such organization has ever existed in that place.

5. Keppel Offshore & Marine Ltd.

On December 22, 2017, Keppel Offshore & Marine Ltd. ("KOM") agreed to pay a total of $422.2 million to authorities in the United States, Brazil, and Singapore to resolve allegations that KOM and its subsidiaries engaged in corruption in connection with Petrobras projects in Brazil. KOM is a Singapore-based company specializing in shipbuilding and repair and offshore rig design, construction, and repair. KOM entered into a Deferred Prosecution Agreement with the DOJ in relation to a charge of conspiracy to violate the anti-bribery provision of the FCPA. KOM also accepted a conditional warning from the Corrupt Practices Investigation Bureau in Singapore. Keppel Offshore & Marine, USA Inc. ("KOM USA"), a wholly-owned subsidiary of KOM based in Houston, Texas, pleaded guilty to one count of conspiracy to violate the anti-bribery provisions of the FCPA. Another KOM subsidiary, Keppel FELS Brasil, reached a Leniency Agreement with the Ministério Público Federal in Brazil related to the same conduct.

Under the terms of the DPA, KOM agreed to a penalty of $422.2 million. Of that amount, $4.7 million was paid on behalf of KOM USA, $211.1 million was credited based on amounts agreed to be paid to Brazilian authorities, and $105.6 million was credited based on amounts agreed to be paid to Singaporean authorities.

A former member of KOM's legal department, Jeffrey Chow, previously pleaded guilty for his role in the scheme. Mr. Chow's plea was unsealed alongside the DPA.

a. Bribery Scheme

The DPA and plea agreement describe an approximately 14-year scheme whereby executives and employees from KOM and KOM USA orchestrated the payment of approximately $55 million in bribes related to 13 different projects in Brazil. The bribes were paid to officials from Petrobas, politicians, and political parties (including the Workers' Party) in Brazil. KOM and its related entities accumulated nearly $352 million in business through the scheme.

Starting in or around 2001, and continuing until around 2011, KOM and KOM USA signed a number of agreements with consulting companies owned in whole or in part by a "Consultant" in connection with several different projects related to offshore floating platforms for Petrobras. Although not named in the U.S. charging documents, the Consultant is widely known to be Zwi Skornicki, a Polish-Brazilian engineer who has been charged in Brazil and confessed to paying bribes to various Brazilian officials. Between approximately 2004 and 2014, KOM paid commissions to Mr. Skornicki through his companies' bank accounts both inside the United States and abroad. All or some of the money was then transferred by Mr. Skornicki for the benefit of two Petrobras employees and the Workers' Party. For example, the DPA details schemes in 2005 and 2009 by KOM executives to pay $4.4 million in bribes to a particular Petrobras official and the Workers' Party in order to obtain contracts on portions of two floating platform hull conversion projects (P-53 and P-58). In total, KOM earned contracts on portions of at least

seven floating platform construction or conversion projects as a result of bribes paid through Mr. Skornicki.

Around 2011 or 2012, KOM executives negotiated bribes with a Brazilian official in connection with a project to construct a fleet of ultra-deepwater rigs. Although Petrobras would be the ultimate end user, the project was commissioned by another Brazilian state-owned enterprise, Sete Brasil. KOM again authorized Mr. Skornicki to pay bribes equal to 1% of the contract value (a total of $14.4 million) to specific Petrobras officials and the Workers' Party.

Jeffrey Chow, a senior member of KOM's legal department, was responsible for drafting the contracts that served as a basis for the corrupt payments. For this, Mr. Chow was charged with, and pleaded guilty to, conspiracy to violate the FCPA. During his plea hearing, Mr. Chow acknowledged having ignored red flags and to understanding that company funds were being used to pay bribes to foreign officials. He further acknowledged that he should have refused to draft the contracts that were used to pay bribes and should have resigned if necessary. His plea agreement included a commitment to assist the DOJ in prosecuting KOM and other former KOM executives.

b. Resolution

Under the three-year DPA, KOM received full remediation and cooperation credit, resulting in a 25% reduction off the bottom of the applicable U.S. Sentencing Guidelines' fine range. KOM received the credit as a result of its substantial cooperation with the DOJ, discipline or termination of culpable employees, imposition of approximately $8.9 million in disciplinary financial sanctions on former and current employees, enhancements to internal controls, and commitment to similar cooperation with authorities in Singapore and Brazil. Given KOM's efforts at remediation, the improvements made to its compliance program, and its commitment to report at least annually during the term of the DPA, the DOJ found that it was unnecessary to require retention of an independent compliance monitor. The DOJ found that though KOM contacted the Fraud Section about allegations publicly reported in Brazil prior to the Fraud Section or the U.S. Attorney's Office contacting KOM, the U.S. authorities were already aware of the allegations. KOM therefore did not receive credit for voluntary disclosure.

Under the terms of the DPA, KOM will report no less than annually to the DOJ on its efforts to, among other activities, implement a rigorous compliance program and strengthen internal accounting controls to prevent future violations.

6. Mondelēz International

On January 6, 2017, the SEC imposed a cease and desist order against Cadbury Limited f/k/a Cadbury plc ("Cadbury") and Mondelēz International, Inc. ("Mondelēz"), which had acquired Cadbury in 2010, based on claims that Cadbury and Mondelēz violated the FCPA's books and records and internal accounting controls provisions. Cadbury is a U.K.-based snack food and beverage company with shares traded on U.S. exchanges. Mondelēz is the U.S. food, beverage, and snack manufacturer previously known as Kraft Foods Inc. Mondelēz and Cadbury consented to the order without admitting or denying the SEC's findings, except as to the SEC's jurisdiction and the subject matter of the proceedings. Mondelēz was additionally ordered to pay a $13 million civil penalty.

According to the SEC's findings, Cadbury India, Cadbury's Indian subsidiary, retained a local businessperson as an agent to assist in obtaining licenses and government approval for the expansion of Cadbury India's chocolate manufacturing facility in Baddi, Himachal Pradesh, India. The agent was hired with little or no due diligence and for seemingly no legitimate purpose. Though the agent was nominally hired and paid to assist Cadbury India with obtaining the requisite approvals for the plant expansion, the SEC found that it was, in fact, Cadbury employees who submitted the required license applications.

The SEC alleged that Cadbury performed no due diligence beyond a January 2010 meeting to negotiate a price for the agent's services. The only documents provided by the agent to Cadbury India were five invoices dating from February to July 2010 totaling $110,446 for "providing consultation, arrange statutory/government prescribed formats of applications to be filed for the various statutory clearances, documentation, preparation of files and the submission of the same with govt. authorities." Cadbury India never entered into a formal contract with the agent nor did the agent provide other reports detailing the services provided to Cadbury India. The agent was paid $90,666 and withdrew most of that money from its bank account in cash. Cadbury India received some of the required licenses and approvals for the expansion during this time period.

Mondelēz acquired Cadbury in February 2010 and conducted, in the SEC's own terms, substantial post-acquisition compliance-related due diligence. This due diligence did not, however, identify Cadbury India's relationship with the agent. In October 2010, Mondelēz launched an internal investigation related to the agent. This investigation led to the termination of Cadbury India's relationship with the agent. Mondelēz additionally took extensive remedial actions including implementing Mondelēz's global compliance program at Cadbury, cooperating with the SEC, and conducting a comprehensive review of Cadbury India's use of third parties.

Cadbury India's failure to perform anti-corruption due diligence, monitor its agent's actions, maintain accurate records relating to the services provided by the agent, and maintain an adequate system of internal accounting controls led to the SEC's cease and desist order and civil penalty. Mondelēz's liability stemmed from its 2010 acquisition of Cadbury.

7. Ng Lap Seng

On July 27, 2017, Chinese real estate mogul Ng Lap Seng was convicted in New York federal court on six counts in connection with a scheme to bribe United Nations ("UN") officials to influence the construction of a conference center in Macau. The charges included: one count of conspiracy to violate the FCPA and to commit theft or bribery concerning programs receiving federal funds (18 U.S.C. §666), two counts of violating the FCPA, one count of bribery concerning a program receiving federal funds, one count of conspiracy to commit money laundering, and one substantive count of money laundering. On May 11, 2018, Ng was sentenced to four years of imprisonment and ordered to pay a criminal fine of $1,000,000 and restitution of $302,977.20.

Ng was one of six individuals indicted on October 5, 2015 in connection with the scheme. The other five individuals were John W. Ashe, the 68th President of the UN, Francis Lorenzo, then Deputy Permanent Representative to the UN for the Dominican Republic, Jeff Yin, Ng's assistant, and Yan Shiwei and Heidi Hong Piao, both executives at a non-governmental organization.

According to prosecutors, from 2011 to September 2015, Ng funneled payments to Ashe and Ashe's wife either directly in cash or through NGOs established by Ng. In return, Ashe promoted and advanced formal UN support for the construction of a multi-billion dollar conference center in Macau by Ng's company, the Macau Real Estate Development Company. Ng wanted the UN to establish this center as the permanent site for the annual United Nations Office for South-South Cooperation ("UNOSSC") Expo and other UN events and meetings. In 2012, after Ng paid for the construction of Ashe's basketball court and hired Ashe's wife as a "climate change consultant," Ashe submitted documents to the UN recommending the construction of this center and listed Ng's company as a partner in the initiative.

Prosecutors also alleged that Ng founded at least three NGOs that he used to facilitate his corrupt scheme. Ng appointed Lorenzo as the "Honorary President" to one such NGO and President to another, paying Lorenzo hundreds of thousands of dollars in these roles. In return, Lorenzo helped advance Ng's interest in building the Macau conference center by facilitating communication with and payments to Ashe.

Starting in 2013, Ashe received $20,000 a month as "Honorary Chairman" of an NGO affiliated with Ng and managed by Yan (CEO) and Piao (Finance Director). Yan and Piao used the NGO to funnel hundreds of thousands of dollars to Ashe for the benefit of Ng as well as other Chinese businessmen.

Prosecutors alleged that Ng and Yin frequently travelled with hundreds of thousands of dollars in cash from China to the U.S. Ng and Yin were arrested shortly after arriving in the U.S. from China on a private plane carrying $500,000 in cash.

Yan and Piao pleaded guilty to bribery and money laundering charges in January 2016. Yan was sentenced to 20 months in prison. Piao awaits sentencing. Lorenzo pleaded guilty to bribery and money laundering charges in March 2016. Sentencing is currently scheduled for October 2018. Ashe died in June 2016 while awaiting trial. In May 2017, shortly before the planned start of his trial, Yin pleaded guilty to a single count of conspiracy to commit tax fraud. He was sentenced in February 2018 to 7 months of imprisonment and ordered to pay restitution of $61,674.

8. Orthofix

On January 18, 2017, Orthofix International N.V ("Orthofix") agreed to pay more than $6 million to settle claims by the SEC that Orthofix violated the FCPA's internal controls and books and records provisions. Orthofix is a medical device manufacturer that develops and sells products to treat the human spine and orthopedic conditions and whose shares are publicly traded on the NASDAQ Stock Exchange. The SEC's charges relate to the conduct of Orthofix's subsidiary in Brazil, Orthofix do Brazil ("Orthofix Brazil"). Under the cease-and-desist order, Orthofix agreed to pay disgorgement of just under $3 million, prejudgment interest of over $263,000, and a civil money penalty of just under $3 million. Orthofix also agreed to retain an independent compliance consultant to review and evaluate Orthofix's anti-corruption compliance program for a period of one year.

According to the SEC, between 2011 and 2013, senior personnel at Orthofix Brazil made payments to doctors employed at government-owned hospitals in order to induce them to use Orthofix's products. These payments were improperly recorded as legitimate expenses in Orthofix Brazil's books and records, which are rolled into Orthofix's books and records. According to the SEC, Orthofix failed to

devise and maintain a system of internal controls sufficient to detect and prevent such payments by Orthofix Brazil.

Orthofix's corrupt payments were made both through third-party commercial representatives and through distributors. Orthofix had two methods to make corrupt payments through commercial representatives. First, Orthofix Brazil paid the commercial representatives a commission of between 33% and 45% on sales, a portion of which the commercial representatives paid to doctors making the purchases. Second, Orthofix Brazil paid companies related to the commercial representatives based on fake invoices for services such as marketing that were never actually provided. These funds were then passed on to the doctors.

The former general manager of Orthofix Brazil approved the payments to the commercial representatives and their companies. The former finance director of Orthofix Brazil instructed employees to classify the payments as "administrative expenses." Orthofix Brazil employees openly referred to these payments as "doctors' commissions" and discussed payment percentages, total amounts, and payment instructions for making direct deposits or in-person payments to the doctors.

With the distributors, Orthofix Brazil offered excessive discounts, including discounts of up to 70% in certain instances, with the understanding that the distributors would use the excess profit to make improper payments to the doctors. Orthofix also paid companies associated with distributors for services that were never rendered. These payments were recorded in Orthofix Brazil's books and records as "consulting for sales" expenses. Between 2011 and 2013, Orthofix earned just under $3 million in total profits from these corrupt schemes.

In August 2013, Orthofix self-reported the conduct of Orthofix Brazil as part of Orthofix's obligations under prior FCPA-related settlements with the SEC and DOJ. In 2012, Orthofix entered into a three-year deferred prosecution agreement with the DOJ and a consent to final judgement with the SEC regarding allegations that the company's Mexican subsidiary, Promeca S.A. de C.V., made corrupt payments to employees of a government agency in Mexico. Under the prior SEC settlement, Orthofix was required to self-report to the SEC regarding its compliance program every six months for a two-year term. In July 2015, the DOJ indicated that it was extending the three-year DPA that had been set to expire that month to give the DOJ time to fully evaluate the Orthofix's compliance with its obligations and to further investigate the reported misconduct in Brazil. In September 2015, the DPA was further extended until July 2016, with the DOJ stating that the company's "efforts to comply with the internal controls and compliance requirements of the DPA during the first eighteen months" were "insufficient." Ultimately, however, when the DPA expired on July 29, 2016, the DOJ agreed to dismiss the case and indicated that it would not take further action in connection with the misconduct in Brazil. The SEC decided to bring the new enforcement action against Orthofix.

The SEC's cease-and-desist order highlights Orthofix's cooperation with the SEC's investigation, which included, among other things, conducting a thorough and timely internal investigation, voluntarily producing documents and other information, providing PowerPoint presentations summarizing the company's findings, and assisting in efforts to coordinate SEC witness interviews. The SEC noted that although Orthofix took remedial steps following the resolution of the prior corruption allegations in 2012, Orthofix did not fully implement sufficient measures until after it discovered the conduct in Brazil in late 2013. The SEC noted that while these remedial efforts were delayed, they were ultimately extensive and

included terminating representatives and distributors involved in misconduct, developing and implementing new global accounting policies, establishing an internal audit function and expanding the compliance department, conducting extensive audits of third-party vendors, and revising existing trainings and implementing additional compliance training.

9. SBM

On November 29, 2017, Dutch offshore oil services provider, SBM Offshore N.V. ("SBM"), entered into a Deferred Prosecution Agreement with the DOJ to resolve allegations that SBM engaged in a conspiracy to violate the anti-bribery provisions of the FCPA. The charges pertained to payments of more than $180 million to intermediaries that were used at least in part to bribe foreign officials in Angola, Brazil, Equatorial Guinea, Kazakhstan, and Iraq. Under the three-year DPA, SBM agreed to pay a total penalty of $238 million, including a $500,000 criminal fine and a $13.2 million criminal forfeiture paid on behalf of SBM's U.S. subsidiary, SBM Offshore USA Inc. ("SBM USA"). The total penalty represents a significant discount from the U.S. Sentencing Guidelines fine range of $4.5 billion to $9 billion. According to the DPA, the DOJ took into account the $240 million that SBM paid to the authorities in the Netherlands and the amounts provisioned related to SBM's planned settlement with Brazilian authorities. The DOJ also considered the need to impose a penalty that did not jeopardize the continued viability of SBM.

SBM also agreed to report to the DOJ on the status of the implementation and remediation of its compliance program on an annual basis during the term of the DPA. Based on the remedial steps SBM took and the state of its compliance program, SBM was not required to retain an independent compliance monitor.

SBM USA pleaded guilty to one count of conspiracy to violate the anti-bribery provisions of the FCPA. SBM's former CEO, Anthony Mace, and a former SBM USA executive, Robert Zubiate, each pleaded guilty to one count of conspiracy to violate the anti-bribery provisions of the FCPA.

a. SBM

According to the DPA, between 1996 and 2011, Mace, Zubiate and other SBM executives orchestrated or directed at least $180 million in "commissions" to intermediaries around the world for the purpose of obtaining or retaining business from state-owned oil companies. SBM earned or expected to earn at least $2.8 billion in connection with these payments. In various places, the DPA notes that SBM officials took steps to conceal the illicit behavior. For example, certain information was discussed over personal email, rather than through the executives' SBM email accounts. On other occasions, SBM employees attempted to delete emails and discussed the need to delete or destroy sensitive emails.

i. Angola

According to the Statement of Facts in the DPA, between 1997 and 2012, SBM paid bribes, both directly and through a sales agent, to officials at Angola's state-owned oil company, Sociedade Nacional de Combustíveis de Angola, E.P. ("Sonangol"), and its wholly-owned U.S. subsidiary, Sonangol USA Co. ("Sonusa"). SBM made commission payments to its sales agent, a former SBM executive, to a bank account in Switzerland knowing that at least part of these funds would be paid to Sonangol and Sonusa officials. SBM also made direct payments to bank accounts and shell companies beneficially owned by

the officials, even though the companies owned by these officials provided no services to SBM. According to the DPA, between 2007 and 2011, SBM paid more than $14 million in "commissions" to shell companies owned by Sonangol and Sonusa officials.

SBM also provided "things of value" to Sonangol officials in the form of gifts, travel, entertainment, and jobs for relatives. For example, in 2000, SBM hired the daughter of a Sonusa official as a cashier, overpaying her for work and paying part of her rent. In addition, SBM USA hired the son of a Sonangol official as an intern, a position that he maintained for four years despite poor performance.

ii. Brazil

From 1996 until around 2012, SBM paid bribes through a Brazilian sales and marketing agent to a number of employees of Petróleo Brasileiro S.A. ("Petrobras"), the Brazilian state-owned oil and gas company. At the sales agent's request, SBM paid the agent's commissions into two different bank accounts, one in Brazil and one in Switzerland in the name of the agent's shell company. The agent then transferred a portion of the Swiss-based funds to the Petrobras officials. For example, in February 2007, SBM wired $601,321 to a bank account in Switzerland in the name of the marketing and sales agent's shell company. Less than a month later, the marketing and sales agent wired more than $500,000 to a different bank account in Switzerland under the control of a Petrobras official.

iii. Equatorial Guinea

SBM used the same sales agent that it retained in Angola to make improper payments to employees of the Republic of Equatorial Guinea's Ministry of Mines, Industry and Energy ("MMIE") and Petroléos de Guinea Ecuatorial ("GEPetrol"). Between 2008 and 2012, SBM paid commissions of tens of millions of dollars to this sales agent to a Swiss bank account. The agent then transferred a portion of these funds to employees of MMIE and GEPetrol. SBM also provided gifts, travel and entertainment to these officials. On one occasion, SBM employees discussed shipping a luxury car from Belgium to a GEPetrol official.

iv. Kazakhstan

From 2003 until around 2009, SBM used two sales intermediaries to pay bribes to employees of KazMunayGas, Kazakhstan's state-owned oil and gas company. One of these sales agents was based in Monaco and received payments from SBM into its accounts in Monaco. SBM intended for the agent to pass on a portion of these payments to KazMunayGas officials. The other sales agent was based in Milan and would receive payment into two accounts: one in Italy and the other in Switzerland held in the name of a shell company. SBM intended that the sales agent would pass on a portion of the payments made in Switzerland to employees of a subsidiary of an Italian oil and gas company that operated the Kashagan oil field.

v. Iraq

In Iraq, SBM retained the same Monaco-based sales agent that it had used in Kazakhstan. SBM paid the sales agent commissions between 2009 and 2012 that it intended, at least in part, to be used as bribe payments to Iraqi government officials, including employees of the South Oil Company, an Iraqi state-owned oil company.

b. Anthony Mace and Robert Zubiate

Anthony Mace, SBM's Chief Executive Officer from 2008 to 2011, pleaded guilty on November 9, 2017 to one count of conspiring to violate the anti-bribery provisions of the FCPA. Mace was also an executive of SBM USA and a member of the board of directors of SBM USA. According to Mace's plea agreement, at the time he became CEO of SBM in 2008, he joined in an ongoing conspiracy to make improper payments to employees of Petrobras, Sonangol and GEPetrol by authorizing and approving payments. In particular, he approved payments when he was aware that there was a high probability that they were improper and deliberately avoided learning that certain payments, including those that he authorized and approved, were improper. According to the plea agreement, in one instance, Mace was in possession of a spreadsheet reflecting over $16 million in payments to five individuals that would be paid through a third party. Mace knew that these individuals were either Equatorial Guinean officials or persons receiving money on behalf of such officials, but nevertheless authorized five transfers from an account in the United Kingdom, through an account in the United States, to a Swiss bank account controlled by the third party. Mace was also aware that payments to SBM's sales agent in Brazil would be paid in part to Swiss accounts held in the name of shell companies. The plea agreement notes that Mace deliberately avoided learning the identities of the ultimate recipients of those payments, who were in fact employees of Petrobras. On September 28, 2018, Mace was sentenced to 36 months in prison and ordered to pay a fine of $150,000.

Robert Zubiate was a sales and marketing executive for SBM USA from around 1990 until 2016. He was responsible for the Latin American division of the company from 1990 until around 2008. On November 6, 2017, Zubiate pleaded guilty to one count of conspiracy to violate the anti-bribery provisions of the FCPA. According to the criminal information filed against Zubiate, he was actively involved in the scheme to bribe employees of Petrobras in Brazil. Zubiate, along with other executives, caused SBM to pay the Brazilian sales and marketing agent, knowing that the intermediary would then pass on portions of those payments to Petrobras personnel. Zubiate also directly received inside information concerning Petrobras's bidding process from the sales and marketing agent and then passed on this information to other SBM and SBM USA employees. The information also notes that, between 1996 and 2011, Zubiate received at least $5.5 million in kickbacks from the sales and marketing agent. On September 28, 2018, Zubiate was sentenced to 30 months in prison and ordered to pay a fine of $50,000.

c. Related Enforcement

SBM's agreement with the DOJ, as well as the cases against Mace and Zubiate, are the most recent enforcement actions stemming from long-running investigations into SBM's conduct by U.S., Dutch and Brazilian authorities. The investigations began when SBM self-reported to authorities in 2012 that an internal investigation had found evidence of misconduct. In 2014, SBM entered into a $240 million out-of-court settlement with the Dutch Public Prosecutor's office (Openbaar Ministerie) in relation to the conduct in Angola, Brazil, and Equatorial Guinea. At the time, the DOJ declined to bring an enforcement action against SBM after finding that there was no apparent basis for U.S. jurisdiction over the matter. The DOJ, however, reopened its investigation in 2016 after learning that Zubiate, who was based in the U.S. and employed by SBM USA, managed a significant portion of the corrupt scheme and engaged in corrupt conduct within the U.S.

On March 17, 2015, SBM entered into a Memorandum of Understanding with the Office of the Attorney General (Advocacia Geral da Uniao) in Brazil setting the framework for a potential settlement with the Attorney General and the Federal Controller-General (Controladoria Geral da Uniao). On July 15, 2016, SBM CEO, Bruno Chabas, and board member, Sietze Hepkema, also entered into an agreement with the Public Prosecutor's office. Finally, in July 2018, SBM entered into a leniency agreement with Brazil's Attorney General, the Ministry of Transparency and Comptroller's General Office, and Petrobras. Under the settlement, SBM agreed to pay nearly $150 million in fines and compensation for damages, to forgo and repay performance bonuses worth approximately $180 million, and to report on the status of its compliance efforts for three years.

10. Sociedad Química y Minera de Chile

On January 13, 2017, Sociedad Química y Minera de Chile ("SQM"), a Chilean chemicals and mining company, entered a deferred prosecution agreement with the DOJ in connection with violations of the FCPA's internal controls and books and records provisions. Under the DPA, SQM agreed to pay a criminal penalty of $15,487,500. On the same day, the SEC issued an administrative cease and desist order as part of a settlement with SQM related to the same conduct. As part of its settlement with the SEC, SQM agreed to pay a $15 million civil penalty.

SQM is an "issuer" within the meaning of the FCPA on account of having shares of its stock listed on the New York Stock Exchange in the form of American Depository Shares. Neither the DOJ nor the SEC alleged any other U.S. nexus in the case, which focused solely on the Chilean company's conduct in Chile.

According to the DOJ and SEC, between 2008 and 2015, SQM failed to maintain adequate internal controls on discretionary funds for the office of the CEO. These funds were earmarked for travel expenses, publicity, consulting, and advisory services as allocated by SQM's CEO. Instead, SQM employees, including a senior executive, used fictitious invoices and contracts to transfer these funds to Chilean politicians, political candidates, and other politically exposed persons ("PEPs"). In total, between 2008 and 2015, SQM paid approximately $14.75 million to PEPs and related individuals and entities from the CEO's discretionary fund.

According to the DPA, on at least two occasions, SQM made payments to Chilean officials through donations to foundations supported by the officials, sometimes in direct response to a request from the officials themselves. At least one of the officials, whose foundation received a $16,000 donation in 2014, had indirect influence over SQM's business in Chile.

Court documents indicate that SQM also created false invoices for payments to vendors solely to disguise payments made directly to Chilean officials, their staff, or their family members. SQM employees created fictitious vendors to disguise the destination of the payments or made invoices to vendors for fictitious services. For instance, in 2009, an SQM executive directed SQM to pay approximately $11,000 on an invoice for "financial services," which was submitted by the sister-in-law of a Chilean government official. No such services were rendered and the invoice was used solely to disguise a payment to a Chilean senatorial campaign. On other occasions, SQM paid invoices connected to a particular Chilean official for "communications advice" or "consulting services" without making any effort to obtain evidence that such services were rendered.

According to the DOJ and SEC, SQM failed to conduct due diligence on vendors or to check that the prices being charged were reasonable for the services listed on the invoices. During a 2014 internal audit, SQM identified several payments from the CEO's discretionary fund to vendors that had connections to PEPs. The internal audit department recommended that the contracts with these vendors be terminated and for additional controls to be put in place. Despite these findings, which were summarized for the board of directors, SQM failed to implement adequate controls on the CEO's discretionary funds and the payments to PEPs continued for an additional six months.

SQM initiated an internal investigation in 2015 after Chilean tax authorities raised questions and the Chilean press ran articles on the matter. As a result of the investigation and its findings, SQM fired its CEO, strengthened its internal compliance and ethics policies, implemented a new accounting oversight system, and reported the potential FCPA violations to the DOJ and SEC.

As a result of SQM's cooperation with the DOJ, SQM's criminal penalty represents a 25% reduction off of the low end of the Sentencing Guidelines. Under current DOJ policy, this is the maximum reduction allowed for a company that did not self-disclose the violation. Despite the fact that SQM disclosed the findings of its internal investigation to the DOJ, the DOJ concluded that SQM did not voluntarily disclose the violations because the internal investigation was prompted by external influences, in particular the Chilean press articles and the inquiries from Chilean tax authorities.

In addition to the financial penalties, SQM also agreed to retain an independent compliance monitor for a period of two years. The DOJ noted that a two-year monitorship was appropriate rather than a three-year monitorship due to the significant steps already taken by SQM to enhance its internal controls and policies and given the size and risk profile of the Company.

11. Colin Steven (Embraer)

On December 21, 2017, Colin Steven, a former Embraer S.A. ("Embraer") sales executive, pleaded guilty to seven felony charges in the Southern District of New York related to his involvement in a scheme to bribe an employee of Saudi Aramco in order to secure the sale of Embraer aircraft to Saudi Aramco.

Mr. Steven, a British national, served as a Regional Vice President in Embraer's Executive Jets Division until December 2013 and was responsible in that position for generating sales in the Middle East. Mr. Steven admitted in court that from November 2009 through April 2011, he and others in Embraer management paid Mazen Snobar, a Saudi Aramco employee, to secure the sale of three new executive jet aircraft to Saudi Aramco. While Aramco originally intended to purchase used aircraft, Mr. Steven admitted that Mr. Snobar agreed not only to award the sale contract to Embraer but to purchase new rather than used aircraft. In return, Mr. Steven and others arranged for Mr. Snobar to receive $550,000 per aircraft in kickbacks, a total of $ 1.65 million.

On March 15, 2010, Embraer and Aramco signed the purchase agreement for three new Embraer jets for approximately $93 million. The payments to Mr. Snobar were reportedly made from Embraer's U.S. subsidiary—Embraer Representations LLC ("Embraer RL")—through a South African intermediary that delivered no services to Embraer and acted solely as a pass-through to disguise payments to Mr. Snobar. Embraer RL ultimately paid more than $1.6 million from its New York bank account to this South

African intermediary. The intermediary then passed on $1.4 million to Mr. Snobar through another intermediary. Mr. Steven also admitted that he arranged for the South African intermediary to redirect approximately $130,000 of fraudulent payments back to Mr. Steven as a kickback.

Mr. Steven pleaded guilty to: (i) conspiracy to violate the FCPA, (ii) violation of the FCPA's anti-bribery provisions, (iii) conspiracy to commit wire fraud, (iv) wire fraud, (v) conspiracy to launder money, (vi) money laundering, and (vii) providing false statements to the FBI when questioned in December 2014 about wire transfers made to the South African intermediary. A sentencing hearing is scheduled for October 24, 2018. Mr. Steven has agreed to forfeit all proceeds traceable to his offenses, including $44,000 in sales commissions he received in March and November 2010 based on the sale of the three new aircraft to Aramco and the $130,000 he retained as part of the kickback scheme.

In October 2016, Embraer reached a $205 million global settlement with the DOJ, SEC, and Brazilian authorities related to corrupt practices by Embraer employees and officers in the Dominican Republic, Saudi Arabia, Mozambique, and India (*see* Hughes Hubbard FCPA & Anti-Bribery Compendium, "Embraer"). The charges against Mr. Steven arose out of his involvement in the Embraer scheme in Saudi Arabia. Mr. Steven's plea revealed that he was the employee known in Embraer's settlement as "Executive B."

12. Mahmoud Thiam

On May 3, 2017, Mahmoud Thiam, a former Minister of Mines and Geology in the Republic of Guinea, was convicted in the U.S. District Court for the Southern District of New York of engaging in a monetary transaction with criminally derived property and laundering money in the United States. The charges centered around $8.5 million that Thiam received from executives of China International Fund Ltd. ("CIF") and China Sonangol International Ltd. ("China Sonangol") (collectively, "Chinese Conglomerate") in return for facilitating an agreement between the Republic of Guinea and the Chinese Conglomerate for exclusive mining rights to large portions of the country's valuable mining reserves.

Thiam, a United States citizen born in Guinea, became Minister of Mines and Geology for the Republic of Guinea in 2009. Thiam played a significant role in granting mining permits to corporations that wanted to invest in mining operations in the Republic of Guinea. His position was especially influential when he took office in 2009 because the country's military dictatorship, which had taken power in 2008, needed private investors to offset a severe shortage of money.

In his capacity as Minister of Mines, Thiam proposed a partnership between the Republic of Guinea and the Chinese Conglomerate. He was the principal negotiator of the deal, which resulted in an agreement, signed on October 10, 2009, granting the Chinese Conglomerate exclusive rights over a large portion of the valuable investment in gold, diamond, bauxite, and iron.

Two weeks before the agreement was signed, Thiam opened a bank account in Hong Kong. His application to open the account failed to disclose his status as a government official for the Republic of Guinea. Instead, he listed himself as a French National and a self-employed consultant. From September 2009 to November 2010, Thiam received close to $8.5 million in monetary transfers from executives of the Chinese Conglomerate. The first of these payments, $3 million, was received in his Hong Kong account two weeks before the agreement was finalized.

Thiam gradually transferred large portions of these funds to the United States. He purchased a $3.5 million 30-acre estate in New York, paid for his children's private Manhattan preparatory schools, and bought a $46,000 piano. According to evidence presented at trial, Thiam took great efforts to conceal the source of the funds for these purchases. For example, he used a Mozambican company to purchase his home, funneling the money for the down payment through a separate Malaysian entity. New York property records confirmed that Thiam was the actual beneficial owner of the estate purchased by the Mozambican company.

Thiam also tried to conceal the sources of his funds and his position as Minister of Mines from the IRS and U.S. banks in which he set up accounts. When contacted by a compliance officer of the New York bank where he transferred $1.3 million, Thiam claimed that he earned the money through business transactions and consulting jobs. He also gave false statements to a second New York bank, telling an employee that he was the chairman of a private mining and natural resources consulting company. Additionally, Thiam's 2009 federal tax returns listed him as a "private banker" for the Ministry of Mining in the Republic of Guinea and his 2009 income as $13,498. In his 2010 returns, Thiam reported $5.8 million income from consulting jobs, and he claimed ownership interests in ten corporations conducting mining operations in Guinea.

Thiam was indicted on January 19, 2017. He was charged with one count of conducting transactions with criminally derived property and one count of money laundering. During the trial, Thiam argued that the funds were a loan from Sam Pa, a Chinese business tycoon allegedly connected to China International Fund. The trial lasted seven days and on May 3, 2017, the federal jury found Thiam guilty of accepting illegal money and laundering it in the United States. Thiam's motion for a new trial was denied on July 11, 2017. On August 25, 2017, Thiam was sentenced to seven years in prison with three years of supervised release. He was also ordered to forfeit $8.5 million.

13. Telia Company AB

On September 21, 2017, Telia Company AB ("Telia"), a Swedish telecommunications company formerly known as TeliaSonera, agreed to pay a total of $965 million as part of a global bribery resolution with DOJ, the SEC, and the Public Prosecution Service of the Netherlands.

Between 2006 and 2010, Telia paid over $331 million in bribes to an Uzbek government official who was a close relative of Uzbekistan's President, Islam Karimov. According to widespread media reports, this Uzbek government official was Islam Karimov's daughter, Gulnara Karimova. During the relevant period, Ms. Karimova had substantial influence over the Uzbek Agency for Communications and Information ("UzACI), the government agency that regulated the Uzbek telecommunications sector.

The allegations against Telia are similar to those made against VimpelCom Ltd., the Amsterdam-based multinational telecommunications company that entered into its own global resolution with U.S. and Dutch authorities in 2016 to resolve allegations that it bribed Ms. Karimova (*see* Hughes Hubbard FCPA & Anti-Bribery Compendium, "Vimpelcom").

a. Bribery Scheme

Telia engaged in a long-running bribery scheme to operate in the Uzbek telecommunications market. Around 2006, Telia identified Coscom LLC, a telecommunications company with existing

operations in Uzbekistan, as an acquisition target and an entry point for Telia into the Uzbek market. In order to secure Ms. Karimova's support for Telia's entry into the Uzbek market, Telia agreed to sell a 26% stake in "Telia Uzbek," the holding company that was purchasing Coscom, to a Gibraltar-based company known as Takilant Ltd. ("Takilant") for $50 million. Takilant was beneficially owned by Ms. Karimova through an associate. In addition to the sale, Telia agreed to pay Takilant $80 million in exchange for Takilant providing licenses, 3G frequencies and number blocks to Coscom. Takilant was also granted an option to sell its stake in Telia Uzbek after two years for a minimum price that would guarantee a significant additional profit. The sale and payment were conditioned on Ms. Karimova acquiring the regulatory assets for Coscom through a Takilant wholly-owned subsidiary.

The SEC alleged that Telia managers knew that the 3G frequencies could be obtained directly from UzACI for no upfront payment. Moreover, according to the DOJ and SEC, certain Telia managers knew that Uzbekistan did not allow the transfer of 3G frequencies between private parties. Nevertheless, Telia agreed that Takilant's subsidiary would obtain the licenses and then repudiate them so that they could be reissued to Coscom.

In November 2007, Takilant's Uzbek subsidiary received the 3G frequencies from UzACI. The following month, Takilant's Uzbek subsidiary repudiated the frequencies, which were then reissued to Coscom. Telia and Takilant then carried out the sale and consulting arrangements as previously agreed. Telia paid Takilant $80 million for licenses, 3G frequencies and number blocks, and Takilant paid Telia $50 million for a 26% stake in Telia Uzbek. In essence, Takilant received $30 million, a 26% stake in Coscom, and the right to sell the stake at a much higher price at a later date.

In 2010, Telia agreed to repurchase 20% of Telia Uzbek's shares from Takilant for $220 million. As a result, Takilant and Ms. Karimova realized a profit of approximately $181.5 million on this portion of the initial investment. Telia also agreed that if Takilant remained a shareholder in Telia Uzbek for at least another three years, the floor price for its remaining 6% stake would be $50 million (thus providing for an additional profit of $38.5 million for this portion of the initial investment). According to the DOJ and SEC, Telia provided these significant profits to Ms. Karimova as bribes to ensure her continued support in obtaining licenses and otherwise supporting Telia's operations in Uzbekistan.

In addition to this overarching scheme, Telia also funneled money to Ms. Karimova using Takilant and other companies owned by Ms. Karimova on numerous occasions, generally through sham consulting arrangements. Telia typically made these payments to secure additional frequencies and licenses and other telecommunications assets issued by regulatory bodies. For example, in 2008 Telia paid $9.2 million to Ms. Karimova through Takilant to obtain a number series of one million numbers and a network code.

In total, through these and other arrangements, Telia paid over $331 million in bribes to Ms. Karimova, and realized profits of approximately $457 million from its Uzbek operations.

b. Global Settlement

Telia entered into a three-year DPA with the DOJ in connection with a criminal information charging Telia with one count of conspiracy to violate the anti-bribery provisions of the FCPA. In addition, Coscom pleaded guilty in connection with a one-count criminal information charging it with conspiracy to violate the anti-bribery provisions of the FCPA.

Under the terms of the DPA, Telia agreed to a total criminal penalty of $548.6 million, including a $500,000 criminal penalty and $40 million forfeiture on behalf of Coscom. The DOJ agreed that the total amount payable to the U.S. Treasury would be offset by the $274 million fine Telia agreed to pay to the Public Prosecution Service of the Netherlands related to the same conduct. As a result, Telia agreed to pay $274.6 million to the U.S. as a criminal penalty and forfeiture. Telia also agreed to continue to cooperate with the DOJ's and other enforcement authorities' ongoing investigation into this matter.

The total criminal penalty of $548.6 million represents a 25% discount off the bottom of the U.S. Sentencing Guidelines fine range, the highest allowed discount under current DOJ policy for conduct that was not voluntarily disclosed. Telia received full credit for cooperating with the DOJ's investigation, including by conducting its own thorough internal investigation. Telia also undertook extensive remedial measures, including terminating individuals involved in the misconduct, creating a new and robust compliance function, implementing a comprehensive anti-corruption compliance program, and overhauling the company's corporate governance structure.

The DOJ also noted that it has filed civil complaints seeking the forfeiture of more than $850 million held in bank accounts in Switzerland, Belgium, Luxembourg and Ireland, which constitute bribe payments made by VimpelCom, Telia, and a third telecommunications company.

Telia resolved the SEC's allegations through a settled administrative order in which the company neither admitted nor denied the SEC's claims that it violated the anti-bribery and internal accounting controls provisions of the FCPA. Under the administrative order, Telia agreed to total disgorgement of ill-gotten gains of $457 million. Recognizing the global nature of the resolution, the SEC agreed to offset the total disgorgement payment in several ways. First, the total disgorgement amount was offset by the $40 million forfeiture paid by Telia on behalf of Coscom as part of Telia's DPA with the DOJ. Half of the remaining $417 million (or $208.5 million) would be payable to the SEC within ten days of the SEC Order. The SEC agreed that the remaining $208.5 million would be offset by any confiscation or forfeiture Telia is required to pay to Dutch or Swedish authorities related to the same conduct.

The SEC indicated that Telia cooperated with the SEC's investigation and had taken certain remedial measures, both before and during the SEC's investigation. These remedial measures included replacing relevant members of its board and adopting and implementing a new compliance program. As with the DOJ, Telia also agreed to continue to cooperate with the SEC's ongoing investigation, as well as all related investigations, litigation and other proceedings.

Although Telia committed to continue to implement a compliance and ethics program designed to prevent violations of the FCPA, Telia was not required to retain a corporate compliance monitor or file regular reports with the DOJ or SEC regarding the status of its compliance program.

14. Zimmer Biomet

On January 12, 2017, Zimmer Biomet Holdings Inc. ("Zimmer Biomet"), the name given to Zimmer Holdings Inc. after its 2015 acquisition of Biomet Inc. ("Biomet"), settled charges with the DOJ and SEC for conduct that occurred in Brazil and Mexico between 2008 and 2013. Zimmer Biomet entered into a deferred prosecution agreement with the DOJ to resolve a charge that the company violated the internal controls provisions of the FCPA and consented to a cease-and-desist order filed by the SEC in

connection with charged violations of the anti-bribery, books and records, and internal controls provisions of the FCPA. In total, Zimmer Biomet agreed to pay approximately $30.5 million in fines, disgorgement, and interest.

Biomet had previously settled FCPA charges with the DOJ and SEC in March 2012, which resulted in a fine and the imposition of a compliance monitor. In 2013, while still operating under the March 2012 DPA with the DOJ, Biomet learned of additional potential FCPA violations that it disclosed to both agencies and its independent monitor in April 2014 and that ultimately gave rise to the 2017 settlements.

a. Violations in Brazil and Mexico

According to admissions by Zimmer Biomet and findings by the SEC, between 2009 and 2013, Biomet knowingly continued to use a distributor in Brazil that had previously paid bribes on Biomet's behalf, as initially discussed in the 2012 DPA. Additionally, between 2008 and 2013, Biomet's indirect but wholly-owned subsidiary Biomet 3i Mexico S.A. de C.V. ("Biomet 3i Mexico") used third-party customs brokers that bribed Mexican customs officials to secure the import of unregistered or improperly labeled Biomet products. During this time, Biomet knowingly failed to implement and maintain internal accounting controls to detect and prevent bribery by its agents, and did not conduct proper due diligence on its potential agents and business partners. According to SEC findings, Biomet also engaged in bribery and falsely recorded improper payments as legitimate expenses, in violation of the FCPA's anti-bribery and books and records provisions, respectively.

i. Conduct in Brazil

In Brazil, Biomet discovered in 2008 that a distributor ("Prohibited Distributor") had paid bribes on Biomet's behalf. Biomet senior management prohibited Biomet from conducting further business with the Prohibited Distributor and the relationship was formally terminated in May 2008. In June 2009, Biomet and the Prohibited Distributor entered into a written agreement barring the Prohibited Distributor from "directly or indirectly" assisting in the sale of Biomet products.

However, beginning in 2009, Biomet used an authorized distributor ("Authorized Distributor"), which Biomet knew was affiliated with the Prohibited Distributor, in order to continue doing business with the Prohibited Distributor. Biomet's failure to implement internal accounting controls, policies, and procedures to prevent or detect bribery allowed this arrangement to continue until approximately 2013.

The relationship with the Authorized Distributor continued even after an internal audit from late 2009 and early 2010 identified the connection between the Authorized Distributor and the Prohibited Distributor. In a draft memorandum, one of Biomet's internal auditors noted the Prohibited Distributor's ownership interest in the Authorized Distributor and recommended that Biomet take steps to ensure that the connection between the Authorized Distributor and the Prohibited Distributor was separated. A Biomet executive subsequently removed this statement from memorandum, thereby ensuring that the recommendation was omitted from the final report.

In April and May 2010, the attorney of the Authorized Distributor's co-owner contacted a Biomet executive ("Biomet Executive") to inform Biomet that the Prohibited Distributor had taken control of the

Authorized Distributor. In response to a query from Biomet executives, the Prohibited Distributor's attorney denied that the Prohibited Distributor was involved in the operations of the Authorized Distributor or the sale of Biomet products. Biomet Executive took no followup actions to determine whether the Prohibited Distributor had any role in the Authorized Distributor's operations. However, in May 2010, a Biomet managing director circulated a presentation stating that "[Authorized Distributor] = [Prohibited Distributor]." Biomet executives continued to meet with the owner of the Prohibited Distributor and in June 2010, the Prohibited Distributor entered into a consulting agreement with the Authorized Distributor for services related to the sale of Biomet products.

Finally, in July 2010, Biomet learned that the Authorized Distributor faced import restrictions in Brazil, limiting it to $150,000 worth of imported product every six months. Biomet Executive authorized a workaround solution in which the Prohibited Distributor would import products directly into Brazil on behalf of the Authorized Distributor. The Authorized Distributor placed orders directly with Biomet, but paid the Prohibited Distributor in cash to cover the products as well as customs and duties costs. The Prohibited Distributor then used the cash in part to cover those costs, transferred the remainder to a private bank account, and wired payment for the products to Biomet from that personal account. The SEC found that Biomet credited the payments to invoices issued to the Authorized Distributor, despite knowing that the funds went to and through the Prohibited Distributor.

In all, Biomet netted roughly $3,168,000 from sales of its products through the Prohibited Distributor and the Authorized Distributor from 2009 through 2013, including from sales of products imported for the Authorized Distributor by the Prohibited Distributor.

ii. Conduct in Mexico

From 2009 to 2010, Biomet failed to respond to red flags regarding the use of customs brokers in Mexico. In particular, in February 2009, Biomet Executive conducted a compliance analysis of a Biomet subsidiary in Mexico. This analysis resulted in the termination of the subsidiary's relationship with a high-risk consultant that had expedited shipments of products with registration issues. Although Biomet 3i Mexico had also previously used the same consultant, Biomet failed to implement controls that would have prevented the use by Biomet 3i Mexico of similarly high-risk third parties.

Subsequently, in 2010, Biomet 3i Mexico encountered difficulty importing its products from the United States to Mexico via the Mexico City airport because the products were incorrectly labeled, omitted mandatory "country of origin" markings, and lacked valid Mexican product registrations. To work around this problem, Biomet 3i Mexico engaged a Mexican customs broker ("Mexican Customs Broker") to transfer improperly labeled and unregistered products across the border illegally through sub-agents. Biomet 3i Mexico was aware that Mexican Customs Broker would use its sub-agents to bribe border officials.

As part of its scheme, Mexican Customs Broker provided separate invoices to Biomet 3i Mexico for services rendered by its sub-agents. Biomet 3i Mexico paid the sub-agents directly but recorded the transfers as payments to Mexican Customs Broker. Zimmer Biomet admitted in its DPA that, between 2010 and 2013, Biomet 3i Mexico paid approximately $980,774 to the Mexican customs broker in connection with importing Biomet 3i products to Mexico. The SEC found that Biomet paid Mexican Customs Broker $549,000 and its sub-agents $981,000. In all, between 2010 and 2013 (or 2008 and

2013 under the SEC's findings), Biomet 3i Mexico earned approximately $2,652,100 in profits from transactions involving Mexican Customs Broker.

b. Settlement Terms

As a condition of its three-year DPA with the DOJ, Zimmer Biomet agreed to pay a criminal fine of $17.46 million, analyze its compliance program and improve it where necessary, and retain an independent compliance monitor. It also agreed that its subsidiary JERDS Luxembourg Holding S.a.r.l. ("JERDS"), the direct holding company of Biomet 3i Mexico, would plead guilty to a single count of violating the FCPA's books and records provision. In light of Zimmer Biomet's fine, the plea agreement between the DOJ and JERDS did not contemplate a financial penalty. The DOJ agreed that if the court imposed a financial penalty at sentencing, such penalty would be credited against the $17.46 million to be paid by Zimmer Biomet.

Zimmer Biomet was not granted credit for voluntary disclosure of the violations because, according to the DOJ, certain underlying facts were not disclosed at the time of the prior DPA. Further, under the DOJ's Pilot Program, a disclosure is not considered voluntary if the company is required to make it by law, agreement, or contract, and Biomet's 2012 DPA required Zimmer Biomet to disclose the facts underlying the current DPA. The DOJ did credit Zimmer Biomet with full cooperation with the DOJ's investigation and Zimmer Biomet's commitment to its compliance program. Nevertheless, the DOJ declined to offer any reduction from the bottom of the Sentencing Guidelines fine range. Instead, Zimmer Biomet's $17.46 million penalty sits squarely within the calculated Sentencing Guidelines range of $11.6 million to $23.3 million.

In connection with the SEC's cease-and-desist order, Zimmer Biomet agreed to pay a fine of $6.5 million, $5.82 million in disgorgement, and $702,705 in prejudgment interest.

As part of its agreements with the DOJ and SEC, Zimmer Biomet also agreed to retain a corporate compliance monitor for a period of three additional years.

Although neither the DOJ DPA nor the SEC settlement directly tie Zimmer Biomet's status as a repeat offender to the penalties issued, it may be significant that the DOJ imposed a fine 50% higher than the bottom end of the Sentencing Guidelines, despite having the latitude to reduce the fine by 25% off the bottom end of the range due to Zimmer Biomet's full cooperation in the investigation.

IV. Other FCPA Developments

In addition to the numerous settlements and criminal matters discussed earlier in this Alert, there have been a number of significant developments related to the FCPA, including important civil litigation, and regulatory guidance, among other things. Certain of these developments are discussed herein.

A. Cohen Further Expands Statute of Limitations in Civil Penalty Actions

In July 2018, a U.S. district court in the Eastern District of New York ruled in *SEC v. Cohen* that the five-year statute of limitations under 28 U.S.C. § 2462 on enforcement actions by the SEC applies to injunctive relief. Section 2462 provides that —

> an action, suit or proceeding for the enforcement of any civil fine, penalty, or forfeiture shall not be entertained unless commenced within five years from the date when the claim first accrued if, within the same period, the offender . . . is found within the United States in order that proper service may be made thereon.

The Supreme Court clarified in *Gabelli v. SEC* that the statute of limitations clock under § 2462 begins when a violation of securities law is completed, not when the violation is discovered. As described below, since that ruling, courts have been slowly expanding the application of § 2462 and restricting the ability of the SEC to seek relief for historic securities violations.

i. Declaratory Relief

In May 2016, in *SEC v. Graham*, the 11th Circuit held that § 2462 applies to certain declaratory relief and disgorgement. In *Graham*, the SEC filed a complaint in January 2013 alleging that the defendants had committed securities violations from November 2004 to July 2008. The SEC sought disgorgement, a declaration that defendants had violated securities laws, a civil penalty, and an injunction from any future violations of securities laws. The district court held that the violations had occurred more than five years prior to the complaint and that § 2462 thus prevented the SEC from seeking civil penalties. Moreover, the district court found that the injunctive and declaratory relief sought by the SEC were "nothing short of a penalty" and thus covered by § 2462. Finally, the district court found that disgorgement should also be covered under § 2462 as it qualified as a "forfeiture." Thus, the district court dismissed the complaint.

The SEC appealed the ruling to the 11th Circuit as to the injunctive and declaratory relief and the disgorgement. The SEC argued that these types of relief are not "civil fines, penalties or forfeiture," and that § 2462 should not apply. The 11th Circuit agreed with the SEC that § 2462 does not apply to purely equitable remedies, including the injunctive relief against future securities violations that the SEC was seeking. However, the 11th Circuit upheld the district court's ruling that the SEC's requests for disgorgement and declaratory relief were time-barred. In particular, the 11th Circuit agreed that the declaratory relief that the SEC was seeking—a declaration that defendants had violated securities laws—was backward-looking and would thus operate as a penalty under § 2462. In making this determination, the 11th Circuit looked to *Gabelli,* in which the Supreme Court recognized that civil penalties "go beyond compensation, are intended to punish, [and] label defendants as wrongdoers." The 11th Circuit found that a declaration of liability is similarly intended to punish and label the defendants as wrongdoers.

ii. Disgorgement

In June 2017, in *Kokesh v. SEC*, the U.S. Supreme Court ruled that the statute of limitations imposed by § 2462 applies to claims for disgorgement in SEC enforcement actions, resolving a circuit split on the issue. The SEC brought an enforcement action in 2009 against Charles Kokesh, the owner of two investment-adviser firms, alleging that he had misappropriated $34.9 million from several of his companies between 1995 and 2009, and had caused the filing of false and misleading SEC reports and proxy statements to conceal the misappropriation. The SEC sought disgorgement of the entire allegedly misappropriated sum, including amounts derived from conduct outside the relevant 5-year limitations

period. The district court held that because disgorgement is not a "penalty" within the meaning of § 2462, no limitations period applied. The Tenth Circuit affirmed.

The Supreme Court reversed, resolving a circuit split by holding that when the SEC seeks disgorgement, that remedy qualifies as a "penalty" subject to the five-year statute of limitations imposed by § 2462. The Court reached this conclusion by applying two principles derived from precedent regarding penalties: (i) a remedy qualifies as a "penalty" if it attempts to redress a wrong to the public, rather than a wrong to the individual; and (ii) a pecuniary sanction qualifies as a penalty if it is imposed as a punishment and to deter similar wrongdoing, rather than to compensate an injured party for his loss. As to the first principle, the Court reasoned that the SEC seeks disgorgement for violations committed against the United States rather than an aggrieved individual. As to the second principle, the Court concluded that SEC disgorgement is imposed for punitive and deterrent purposes and, in many cases, is explicitly not compensatory. The Court rejected the government's argument that disgorgement is merely "remedial" and designed to return the defendant to the status quo ex ante, because SEC disgorgement sometimes exceeds the profits the defendant gained as a result of the violation.

iii. Certain Injunctive Relief

In July 2018, in *SEC* v. *Cohen*, the U.S. District Court for the Eastern District of New York held that § 2462 applied to a request for injunctive relief. The SEC filed a complaint in 2017 alleging that the defendants had orchestrated a "sprawling scheme" to bribe various public officials in various African countries in exchange for business for their employer, hedge-fund management firm Och-Ziff Capital Management LLC. The SEC sought civil penalties, disgorgement, and an injunction from any future violations of securities laws. The district court ruled that the violations had occurred more than five years prior to the complaint and that § 2462 thus prevented the SEC from seeking civil penalties or disgorgement pursuant to the U.S. Supreme Court's ruling in *Kokesh*. Further, the district court held that under the reasoning of *Kokesh*, the SEC's requested injunction was time-barred as well. According to the district court, the reasoning of *Kokesh* implied that § 2462 applied to the requested injunction because the SEC sought the injunction to redress "wrongs to the public," not just "wrongs to individuals"; and because the injunction would operate at least in part as a penalty, since it would "mark the defendants as lawbreakers" and "stigmatize them in the eyes of the public." Thus, the district court dismissed the complaint.

The district court's decision was in accord with a similar ruling by the U.S. District Court for the District of New Jersey in December 2017 in *SEC v. Gentile* applying § 2462 to a request for injunctive relief. However, the district court in *Cohen* acknowledged that its decision was in tension with the Eighth Circuit's June 2017 decision in *SEC* v. *Collyard*, in which the court had concluded that the SEC's requested injunction barring the defendant from operating as an unregistered broker was not a § 2462 penalty because it "(1) requires only obedience with the law, (2) is based on evidence of a likelihood to violate that law, and (3) seeks to protect the public prospectively from [the defendant's] harmful conduct rather than punish [him]." (The Eight Circuit reserved decision as to whether an injunction can *ever* be a penalty under § 2462.) According to the Eighth Circuit, although the injunction at issue would likely deter the defendant from violating the securities laws, such deterrence was only an "incidental effect" of the requested injunction, which was therefore not time-barred. The district court in *Cohen* found this reasoning to be at odds with *Kokesh*.

B. FCPA-Related Civil Litigation

The FCPA does not provide for a private cause of action. Nevertheless, enterprising shareholders, employees, competitors, and even foreign governments have sought alternative means to use allegations of bribery as a basis to bring derivative actions, securities class-action suits, suits under the federal Racketeering Influenced Corrupt Organization ("RICO") Act, and whistleblower complaints, among other legal actions.

1. Recent Derivative Actions

a. Background

When a publicly-traded company resolves an FCPA investigation brought by the DOJ or the SEC, or discloses that such an investigation is underway, the company's shareholders can file derivative suits (i.e., suits on behalf of the company, as contrasted to direct shareholder suits pursued on the shareholders' own behalf) under state law. These suits typically allege that the company's board of directors breached its fiduciary duty by failing to implement or adequately monitor the company's anti-bribery controls.

Ordinarily, a prospective plaintiff in a derivative suit must first make a written demand to the board of directors notifying the board of the claimed failure or lapse of internal controls and asking the board to take remedial action, often including a decision to initiate litigation against the alleged wrongdoers. If the board of directors, in the proper exercise of its business judgment, decides not to pursue the shareholder's demand, the board may be protected from liability. Because of this protection, many plaintiffs allege that making such a demand would be futile for a variety of reasons, including the claim that the board's alleged alignment with the company's management prevents it from making an impartial assessment of the shareholder's allegations. Therefore, a plaintiff in a derivative suit must allege with particularity either that (a) the plaintiff has satisfied the demand requirement or (b) the demand requirement should be excused on the basis of futility.

The standard for establishing demand futility can be difficult to meet. To establish that a shareholder demand is futile, plaintiffs generally must show that a majority of a company's board members are unable to impartially consider the demand. *Freuler v. Parker*, 803 F. Supp. 2d 630, 641 (S.D. Tex. 2011). Plaintiffs alleging that a demand is futile because board members face potential liability must show "a substantial likelihood of personal liability…." *Id.* (citing *Aronson v. Lewis*, 473 A.2d 805, 814 (Del. 1984) (internal citations omitted)).

Assuming a non-demanding plaintiff is able to overcome the demand futility hurdle, the plaintiff "must show with particularized facts that the directors *knew* they were not discharging their fiduciary obligations or that the directors demonstrated a *conscious* disregard for their responsibilities such as failing to act in the face of a known duty to act" to establish liability for inadequate oversight. *Freuler*, 803 F. Supp. 2d at 640 (applying Delaware law and citing *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959, 971 (Del. Ch. 1996) (emphasis in original)). Moreover, plaintiffs must further show that "(a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, [they] consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention." *Midwestern*

Teamsters Pension Trust Fund v. Baker Hughes, Inc., Civil Action No. H-08-1809, 2009 WL 6799492, *4 (S.D. Tex. May 7, 2009) (quoting *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006)). The mere fact that a violation occurred is not sufficient to prove bad faith on the part of the directors. *Id.*

b. Recent Notable Dismissed Cases

Plaintiffs in derivative actions shoulder a heavy burden to survive a motion to dismiss and pursue their claims successfully. Indeed, "a breach of [directors'] duty of attention or care in connection with the on-going operation of the corporation's business . . . is possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment." *Freuler*, 803 F. Supp. 2d at 639 (citing *Caremark*, 698 A.2d at 967). Numerous shareholder-derivative actions based on the claim of a director's breach of his or her fiduciary duties in connection with alleged violation of the FCPA have been dismissed for failure to meet the requisite pleading standards. Two recent cases include:

- On June 16, 2017, the Delaware Court of Chancery dismissed a shareholder derivative suit on behalf of Qualcomm, Inc., accusing its directors of not doing enough to prevent FCPA violations that occurred in China between 2002 and 2012. The lawsuit followed Qualcomm's disclosure, in a 2012 SEC filing, that it was being investigated for FCPA violations by the U.S. Attorney's Office for the Southern District of California, and that the company ultimately paid a $7.5 million penalty to the SEC. The shareholder-plaintiffs largely relied on evidence obtained from the U.S. Attorney's Office's investigation.

  Attempting to establish demand futility, the plaintiffs alleged that the defendant directors acted in bad faith by consciously failing to monitor the operation of Qualcomm's internal controls. However, Vice Chancellor Tamika Montgomery-Reeves dismissed the suit, finding that many of the reports and presentations on which the plaintiffs relied to show "red flags" the directors allegedly failed to monitor in bad faith, actually contained the company's remedial plans to address those red flags. The Vice Chancellor therefore concluded that the complaint did not contain sufficiently particularized "allegations [to] suggest that the Qualcomm board consciously disregarded the red flags" and that the plaintiffs "simply s[ought] to second-guess the timing and manner of the board's response to the red flags."[33]

- Och-Ziff Capital Management faced a shareholder derivate suit filed in September 2015 in the New York Supreme Court in New York County for alleged FCPA violations in Africa. The complaint alleged that the board of directors breached its fiduciary duties in connection with the events leading to FCPA investigations by the DOJ and SEC, including allegations that Och-Ziff: (i) extended a $100 million no-interest loan to former President Mugabe of Zimbabwe in exchange for access to platinum reserves; (ii) extended questionable loans in the Democratic Republic of Congo that ultimately allowed it to acquire or control various natural resource assets at below-market value, including several that had been nationalized from foreign investors shortly before their re-sale; and (iii) entered into a hotel deal for the benefit of the now-deceased Libyan leader Muammar Gaddafi after receiving approximately $300 million in investments from the Libya Investment Authority sovereign wealth fund. On September 23, 2016, the court dismissed the case, noting in its decision that the board's

33. *In re: Qualcomm Inc. FCPA Stockholder Derivative Litigation*, C.A. No. 11152-VCMR (Del. Ch. June 16, 2017).

demand review committee adequately investigated the shareholder's complaint over a period of months and, as such, acted in good faith.[34]

c. Recent Notable Settlements

At least one recent derivative suit has resulted in a settlement, which typically require the subject companies to adopt enhanced anti-corruption programs and pay the attorney's fees incurred by the plaintiff-shareholders. In particular, in September 2017, the petrochemical firm Braskem settled a derivative suit filed in the U.S. District Court for the Southern District of New York that claimed that the value of Braskem's American depositary receipts fell by more than 20% after disclosure of the firm's involvement in the Brazilian Petrobras scandal. The plaintiffs claimed that Braskem defrauded shareholders by failing to disclose the payments of millions of dollars in illegal bribes to Brazilian officials in exchange for lower prices on naptha, an important ingredient in petrochemical processing. The order preliminarily approving a proposed settlement of $10 million was approved by Judge Paul A. Engelmayer on September 15, 2017. *See In re Braskem, S.A. Securities Litigation*, No. 15-CV-5132-PAE (S.D.N.Y. Sept. 15, 2017).

2. Class Action Securities Suits

a. Background

In addition to derivative actions, would-be plaintiffs also have the option of bringing class action securities lawsuits pursuant to Section 10(b) of the Securities Exchange Act and SEC Rule 10b-5, which states:

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange, (a) to employ any device, scheme, or artifice to defraud, (b) to make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or (c) to engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.

To state a claim under Section10(b) or Rule 10b-5, a shareholder-plaintiff must allege that the defendant company or directors "made a false statement or omitted a material fact, with scienter, and that the plaintiff's reliance on defendant's action caused the plaintiff's injury." The Private Securities Litigation Reform Act ("PSLRA") heightened this pleading standard, requiring that the complaint must (i) "specify each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, the complaint shall state with particularity all facts on which that belief is formed," and (ii) "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind."

34. *Kumari et al. v. Och et al.*, NO 653016/2015 (N.Y. Sup. Ct. Sept. 20, 2016).

Providing detailed factual allegations that the defendants acted with the necessary scienter has proven to be the most difficult element for plaintiffs to plead sufficiently. To meet the "strong inference" requirement, the United States Supreme Court has required that the facts alleged be cogent and create an inference "at least as compelling as any opposing inference of non-fraudulent intent" that the defendant sought to deceive, manipulate, or defraud.

In 2010, the U.S. Supreme Court made it even more difficult for plaintiffs who acquired shares outside the United States to file claims in U.S. federal courts. In *Morrison v. National Australia Bank*, 130 S. Ct. 2869 (2010), the Court held that Section 10(b) and Rule 10b-5 do not apply extraterritorially, reversing previous federal case law. The Court specified that plaintiffs could only bring such cases if "the purchase or sale is made in the United States, or involves a security listed on a domestic exchange."

b. Recent Notable Dismissed Cases

At least two recent cases have been dismissed where plaintiffs have failed to meet these stringent standards, including:

- Investors in Embraer S.A. American depositary receipts ("ADRs") were successful in certifying a class action in the U.S. District Court for the Southern District of New York, alleging that the Brazilian airplane manufacturer, and certain of its executives, violated Sections 10(b) and 20(a) of the Exchange Act, and SEC Rule 10b-5, by making material misstatements or omissions in the company's SEC filings between 2012-2016—*i.e. after Embraer's alleged violations of the FCPA had ceased and while it was under investigation by the DOJ*. While Embraer's public filings during the class period contained references to its potential liability during the ongoing investigation, the class members alleged that Embraer had, *inter alia*, failed to disclose the scope of its illicit activities and estimate and disclose the profits it might be forced to disgorge in a future settlement with the DOJ. The class members also alleged that Embraer had misrepresented its subsidiaries' involvement in the alleged illicit conduct by referencing those subsidiaries' legitimate business activities in its public filings.

  On March 30, 2018, Judge Berman granted defendants' motion to dismiss, ruling that applicable federal securities laws do not require issuers to "disclose uncharged, adjudicated wrongdoing." He, thus, found that Embraer's public filings during the class year complied with federal securities laws. Clerk's Judgment, *In re Petrobras Securities*, No. 1:14-CV-09662-JSR (S.D.N.Y. June 27, 2018).

- Shareholder plaintiffs filed a putative class action claim against Qualcomm accusing Qualcomm's directors of not doing enough to prevent the FCPA violations (dismissed by the Delaware Chancery Court on June 16, 2017, which found that the putative class had not supported any of its claims that the board acted improperly and neglected its fiduciary duties). *In re: Qualcomm Inc. FCPA Stockholder Derivative Litigation*, C.A. No. 11152-VCMR (Del. Ch. June 16, 2017).

c. Recent Notable Settlements

Despite the substantial pleading threshold burdens and limitations on the FCPA's applicability to conduct occurring outside the United States, several recent class actions have resulted in settlement:

- On October 2, 2018, Och-Ziff agreed to pay $28.75 million to settle a class action lawsuit brought by investors in the Southern District of New York. The suit originated in 2014 when investors sued Och-Ziff claiming that CEO Daniel Och and former chief financial officer Joel Franck violated securities laws when they failed to disclose that Och-Ziff was under investigation for potential FCPA violations. The settlement awaits approval from the court.

- Investors in Petrobras, whose ADRs are listed on the NYSE, filed a December 8, 2014 class action in the U.S. District Court for the Southern District of New York, claiming that Petrobras "made false and misleading statements by misrepresenting facts and failing to disclose a multi-year, multi-billion dollar money laundering scheme" and imputing Petrobras's executives knowledge of the scheme to the company.

  On February 2, 2016, Judge Rakoff granted the plaintiffs' motion to certify two class actions under Federal Rule of Civil Procedure 23(b), the first pursuing claims under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934, and the second pursuing claims under Sections 11, 12(a)(2) and 15 of the Securities Act of 1933. However, on July 7, 2017, the U.S. Court of Appeals for the Second Circuit vacated Judge Rakoff's certification in part, ordering the court to determine whether, under Federal Rule of Civil Procedure 23(b)(3), questions of law or fact common to the putative class predominated over those affecting individual class members. Specifically, the Second Circuit held that the Supreme Court's ruling in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010)—a seminal opinion addressing the extraterritorial reach of U.S. securities laws—required the district court to make findings regarding whether each class member's purchase of Petrobras ADRs—which do not trade on a domestic exchange—showed "markers of domesticity." Thus, the Second Circuit remanded the action to the Southern District of New York in an order requiring Judge Rakoff to determine whether the need to conduct a *Morrison* assessment precluded a finding that Rule 23(b)(3)'s predominance requirement was satisfied.[35]

  On July 27, 2018, Judge Rakoff approved a $3 billion settlement of the plaintiffs' claims, with Petrobras agreeing to pay $2.95 billion and PricewaterhouseCooper agreeing to pay $50 million. The Judge also awarded approximately $200 million in fees.[36]

- On March 25, 2017, Judge John G. Koeltl of the U.S. District Court for the Southern District of New York largely ruled against a motion to dismiss a class action suit relating to Brazil's state-run electric company, Eletrobras. In his ruling, Judge Koeltl found plausible the investors' claims that they were misled by the company's statements made before it revealed that some of its officers were engaged in bribery or bid rigging. In the decision, Judge Koeltl noted that even "as news continued to trickle out about further evidence implicating

35. Order, *In re Petrobras Securities*, No. 16-1914-CV (2d Cir. July 17, 2017).
36. Order, *In re Petrobras Securities*, No. 14-CV-9662 (S.D.N.Y. June 25, 2018)

Eletrobras in the bribery and bid-rigging investigation, Eletrobras repeatedly emphasized and reasserted the strength of its internal controls and its commitment to transparency and ethical conduct." Although Jose Antonio Muniz Lopes, Eletrobras's former CEO, was cleared of all claims of wrongdoing, the court declined to dismiss claims against two other former officers who allegedly acted with scienter in making false disclosures to shareholders.

On August 17, 2018, the court issued an order providing its preliminary approval for a proposed settlement between the parties in the amount of $14.75 million.[37]

d. Recently Filed Actions

i. Actions Against Glencore Plc.

Two seemingly dueling class actions were recently filed against Glencore Plc. ("Glencore") in the U.S. District Courts for the District of New Jersey (July 9, 2018)[38] and the Southern District Court of New York (July 11, 2018).[39] Both allege that Glencore and certain of its executives[40] violated Sections 10(b) and Rule 10-b-5 of the Securities Exchange Act of 1934 and that the identified executive(s) violated Section 20(a) of the same. The complaints center on alleged corruption in the Democratic Republic of the Congo ("DRC") involving Glencore's business partner, Dan Gertler, who was previously implicated in corruption tied to Och-Ziff Capital Management (discussed *supra*).

Glencore, a U.K. company principally based in Baar, Switzerland, is a multinational company engaged in the production, refinement, processing, storage, transport, and marketing of metals and minerals, and energy and agricultural products. On September 30, 2016, a news report indicated that Glencore was reviewing allegations made by the U.S. government regarding the activities of a Glencore business partner in the DRC, which an anonymous source reported to be Gertler. The same article reported that Glencore responded to the news by issuing an official statement that Glencore viewed ethics and compliance "very seriously" and that it was reviewing the information described in the report. The complaints allege that, following its September 2016 statement, Glencore made materially misleading statements in its 2017 and 2018 annual reports by failing to disclose adverse facts pertaining to its activities, which would "reasonably subject it to heightened scrutiny by U.S. and foreign government bodies with respect to…compliance…."

Citing news reports from May 2018 that the U.K.'s Serious Fraud Office was seeking to undertake a full-investigation of Glencore's activities in the DRC, and a July 3, 2018 subpoena issued by the U.S. Department of Justice to a Glencore subsidiary, the complaints allege that the defendants engaged in a scheme or course of conduct whereby they either intentionally or recklessly made various misrepresentations and omissions in their public filings about Glencore's compliance with anti-bribery law. The complaints allege that the putative classes are comprised of purchasers of Glencore's over-the-counter stock between September 30, 2016 and July 3, 2018, who relied on the alleged material misrepresentations and omissions and thus allegedly purchased the stock at inflated prices. The plaintiffs

37. Order, *In re Electrobras Securities Litigation*, NO. 15-Civ-5754 (Aug. 17, 2018).
38. *Church v. Glencore Plc.*, No. 2:18-cv-11477-SDW-CLW (D.N.J July 9, 2018).
39. *Robinson v. Glencore Plc.*, No. 1:18-CV-06286-VEC (S.D.N.Y. July 11, 2018).
40. While the action in New Jersey was asserted against two Glencore executives, Ivan Glasenberg (CEO) and Steven Kalmin (CFO), the New York action does not include Mr. Kalmin as a defendant.

further claim that the defendant-executive(s), having the requisite knowledge and the authority to control Glencore's public filings, caused Glencore to violate federal securities laws by issuing false and/or misleading reports.

ii. In re Veon Ltd. Securities Litigation[41]

On September 19, 2017, Judge Andrew Carter, Jr. of the U.S. District Court for the Southern District of New York held that the putative class action against VEON, Ltd. (formerly d/b/a VimpelCom) could move forward. In February 2016, VEON entered a deferred prosecution agreement with the Department of Justice for FCPA violations related to bribes paid to the president of Uzbekistan's daughter in return for favorable treatment in the Uzbek telecommunications market. The plaintiffs allege that the conduct forming the basis of the FCPA violations led to material misstatements and omissions in the company's SEC filings. The court held that those statements "sufficiently place the reasons for [VEON's] growth in Uzbekistan at issue to make further disclosure necessary." The court further held that the plaintiffs' alleged facts that "gave rise to strong inference of corporate scienter" on the part of VEON's executives.[42]

3. Recent Lawsuits by Foreign Governments and State-Owned Entities

Companies that have resolved charges with the DOJ and SEC occasionally face additional U.S.-based lawsuits from the foreign countries or state-owned entities implicated in the action. While the mere fact that persons acting on behalf of those government entities may themselves have solicited or received the payments in question has not prevented them from bringing suit, courts have appeared reluctant to allow such entities to bring claims when the entities themselves could be considered co-conspirators. Moreover, these types of plaintiffs face the same challenges as typical shareholder plaintiffs in overcoming the stringent pleading standards and *Morrison*'s limitation on the applicability of U.S. securities laws extraterritorially. But if the foreign government or state-owned entity can survive a motion to dismiss, a substantial settlement could be attained.

Additionally, some governments that have chosen to pursue civil claims in the United States in connection with the FCPA have attempted to utilize the federal RICO statute, which prohibits, *inter alia*, the conduct of an enterprise's affairs through a pattern of racketeering activity, and provides a civil cause of action to persons injured by racketeering activity prohibited by the statute. 18 U.S.C. § 1964(d). *See RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090, 2097 (2016). However, in 2016, the Supreme Court ruled that the general presumption against a statute's extraterritorial application requires that a plaintiff asserting a civil RICO claim assert a "domestic injury." *RJR Nabisco, Inc.*, 136 S.Ct.2111. As the cases below indicate, the Court's ruling placed a significant barrier in the way of plaintiffs seeking to assert RICO claims based on alleged violations of the FCPA, which, by their very nature, involve foreign government officials and often occur abroad.

41. *See In re Veon Ltd. Securities Litigation*, No. 15-cv-08672 (S.D.N.Y. 2018).
42. On August 20, 3018, the Southern District of New York dismissed the claims against the individual defendants, ruling that the plaintiffs had failed to properly serve those defendants, that certain of the plaintiffs claims had expired under applicable statutes of limitation and repose, and that the plaintiffs had failed to adequately plead scienter. *In re Veon Ltd. Securities Litigation*, Slip. Op. No. 15-cv-08672 (S.D.N.Y. Aug. 30, 2018).

In early 2018, an entity called PDVSA US Litigation Trust filed a RICO action in the U.S. District Court for the Southern District of Florida on behalf of Venezuela's state-owned oil company against a group of oil brokers, banks, and other defendants, alleging that the defendants had engaged in a 14-year bribery conspiracy designed to rig PDVSA's tendering process in favor of the defendant oil brokers. The lawsuit raises a number of issues commonly implicated in FCPA-related RICO claims, including whether the plaintiffs will be able to assert a domestic injury—as required for civil RICO claims pursuant to the United States Supreme Court's recent ruling in *RJR Nabisco*—as well as unique questions, such as whether the PDVSA trust, ostensibly established for the sole benefit of PDVSA, has standing to assert the RICO claim on PDVSA's behalf. Defendant's Joint Response in Opposition to Plaintiff's Motion for a Preliminary Injunction, *PDVSA US Litigation Trust v. Lukoil Pan Americas LLC*, No. 1:18-CV-20818-DPG (Mar. 26, 2018).

4. Other Recent FCPA-Related Civil Actions

a. EIG Energy Fund XIV, L.P. v. Petroleo Brasileiro, S.A.

EIG Energy Fund L.P. ("EIG"), a Washington D.C.-based fund that had invested (through a Luxembourg-based intermediary) in a Petrobras-managed venture, Sete Brasil Participacoes, S.A., lost approximately $221 million in the wake of Operation Car Wash, which exposed significant bribery within the Brazilian state-owned entity and caused the highly-leveraged venture to collapse as creditors withdrew their support. EIG then sought to recover its losses by pursuing an action in the U.S. District Court for the District of Columbia for fraud, aiding and abetting fraud, and civil conspiracy.

Petrobras responded to the suit by filing a motion to dismiss, arguing that, as an instrumentality of a foreign state, it is immune under the Foreign Sovereign Immunities Act ("FSIA"). The district court denied Petrobras's motion, concluding that Petrobras was not entitled to immunity under the statute's "direct effect" exception because its decision to target American investors had a direct effect in the United States.

On July 3, 2018, the United States Court of Appeals for the District of Columbia affirmed the district court's holding. The D.C. Circuit's ruling rejected two arguments advanced by Petrobras. First, the court rejected Petrobras's argument that its fraud did not cause a direct effect in the United States because the causal chain was broken by the creditors' decision to withdraw from the project. The court reasoned that adopting Petrobras's "but for" approach would immunize the company from the foreseeable effects of its fraud. Second, the court rejected Petrobras's argument that any injury caused to EIG was not direct because it was incurred through EIG's Luxembourg subsidiary. Rejecting this second argument, the court ruled that the effects of a commercial action may be sufficiently direct so as to trigger the FSIA's exception even where the relevant tort's locus is in a foreign country. Order, *EIG Energy Fund XIV, L.P. v. Petrolieiro, S.A.*, No. 17-7067 (D.C. Cir. July 3, 2018).

b. Eley v. General Cable Corporation

Companies may also face additional legal challenges from their own employees as to the exact scope of their fiduciary duties in stewarding those employees' investments in any company-managed retirement plans in the wake of discovering potential FCPA exposure. For, example, in *Eley v. General Cable Corporation*, a plaintiff class comprised of General Cable Corporation ("General Cable") employees

that had invested in a General-Cable-managed retirement fund filed suit in the U.S. District Court for the Eastern District of Kentucky, alleging that the corporation breached its fiduciary duties of prudence, loyalty, and the requirement to monitor by not taking steps to protect those employees' retirement plans from losses tied to the value of the corporation's stock. *Eley v. General Cable Corporation*, No. 2:17-CV-00045-DLB-JGW (E.D. Ky. 2017).

In December 2016, General Cable entered into an NPA and a cease-and-desist settlement with the DOJ and the SEC, respectively. Both settlements were accompanied by factual stipulations, which alleged that General Cable's subsidiaries paid, through third-party agents, somewhere in the range of $13-19 million to government officials in Angola, Thailand, China, Indonesia, Bangladesh, and Egypt, and that these bribes generated profits of over $51 million. Notably, the settlements also indicated that certain General Cable executives had been aware of red flags indicating that those subsidiaries may have been involved in the payment of bribes to government officials. The settlements required General Cable to pay over $82 million ($27 million in penalties and $55.3 million in disgorged profits).

The plaintiffs' claims relied on the Employee Retirement Income Security Act of 1974 ("ERISA") 29 U.S.C. §§ 1104, 1105, 1109, and 1132, and the burden that that statute places on fiduciaries managing ERISA-covered retirement plans.[43] Relying on ERISA's requirement that every ERISA-covered plan designate at least one fiduciary with control over the plan and the statute's own definition of "fiduciary" that includes every person who exercises discretionary authority or control over the management of a covered plan, the plaintiffs argued that General Cable's management of its retirement plan violated the statute.[44] Plaintiffs alleged that:

- The defendants breached their duty of prudence by continuing to allow the covered plan's investment in General Cable stock, despite the fact that the company and its executives knew or should have known that the investment was imprudent as a retirement vehicle because the stock was artificially inflated;

- The defendants breached their duty of loyalty by continuing to allow the covered plan's investment in General Cable stock, in essence putting General Cable's interest before the investor-employees;

- The defendants breached their duty to monitor by failing to ensure that any of the fiduciaries managing the fund had access to the information necessary to act properly within their role as fiduciaries and for failing to monitor those fiduciaries, including by ensuring that the fiduciaries were managing the fund after receiving the necessary information.

On July 23, 2018, the court dismissed each of these claims. First, the court noted that *Dudenhoeffer* requires that plaintiff seeking to state a claim for breach of the duty of prudence to

43. The complaint relied on Supreme Court decisions interpreting ERISA, including *Fifth Third Bancorp v. Dudenhoeffer*, S.Ct. 2459 (2014) (holding that ERISA fiduciaries do not enjoy a presumption of prudence, and that said duty is primary to the fiduciary's execution of an investment plan, including any instruction to invest in securities of the employer-company managing the fund).
44. Section 502(a)(2) of ERISA, codified at 29 U.S.C. § 1132(a)(2), establishes a private right of action for breaches of ERISA-imposed fiduciary duties. Section 409(a), codified at 9 U.S.C. § 1109(a), imposes personal liability on those who breach the statute.

"plausibly allege an alternative action that the defendant could have taken that would have been consistent with the securities laws[,] and that a prudent fiduciary in the same circumstances would not have viewed as more likely to harm the fund than to help it." Reviewing the plaintiffs various arguments, the court ruled that the plaintiffs had not plausibly set out what steps the defendants could have taken that, without the benefit of hindsight, might not have presented decision makers with the possibility of greater losses. For example, the court took issue with the plaintiffs' suggestion that the defendants could have ordered the ERISA-covered fund to stop purchasing General Cable stock upon discovering the relevant FCPA violations, noting the potentially negative signal that such a decision would send to the market about the company's stock.[45]

Second, the court dismissed the plaintiffs' duty of loyalty claim because it was, in part, derivative of the plaintiffs' duty of prudence claim and because the plaintiffs failed to cite to misleading statements made by General Cable in the wake of their discovery of their potential FCPA exposure. Finally, the court dismissed the duty to monitor claim as derivative of the first two claims. Plaintiffs have since filed a notice of appeal.

c. Harvest Natural Resources, Inc. v. Garcia

On February 16, 2018, Harvest Natural Resources, Inc. ("Harvest") filed a complaint against certain individuals associated with PDVSA, asserting claims for violations of RICO, the Sherman Act, and of the Robinson-Patman Act, as well as alleging a RICO conspiracy. *Harvest Natural Resources, Inc. v. Garcia*, No. 4:18-CV-00483 (S.D. Tex. May 11, 2018). Harvest, a formerly publicly traded company based in Texas that engaged in the development and production of oil and gas properties, alleged that the defendants conspired to block Harvest's sale of certain Venezuelan assets to PT Pertamina after Harvest had refused to pay one of the defendants a $10 million bribe. The complaint alleges that the sale was ultimately delayed for four years and executed at a $470 million discount.

The parties are currently engaged in jurisdictional discovery.

d. Atchley v. Astrazeneca U.K. Ltd.

On October 17, 2017, a class action suit was filed on behalf of American service members and their families injured by members of the Iraqi terrorist organization known as Jaysh al Mahdi, or the Mahdi's Army, led by Muqtada al Sadr. *Atchley v. Astrazeneca U.K. Ltd.*, No. 1:17-CV—2136, ¶¶ 49, 193 (D.D.C. October 17, 2017). The complaint's basic allegation is that the defendants—including Astrazeneca, Johnson and Johnson, Pfizer, Inc., GE Healthcare USA Holding, LLC, F. Hoffman-LaRoche Ltd., various of those companies' affiliates, and others—engaged in bribery schemes by making payments in the form of "free goods," providing fictitious after-sale services through third-party agents, and paying commissions to the Iraqi Ministry of Health and the Ministry's state-owned subsidiary, Kimada.

The complaint noted that a number of the defendants or their affiliates had previously reached settlements with the DOJ and the SEC in connection with, *inter alia*, similar bribery schemes perpetrated

45. In rejecting the plaintiffs' argument, the court did not consider the possibility that the decision not to freeze the fund's purchase of General Cable stock was made at multiple points in time and that while a prudent fiduciary might have initially believed that such a freeze could have caused more harm than good, that position may have been less persuasive as the depth of General Cable's FCPA violations became known within that company.

during the course of the Iraqi Oil-For-Food Program. The plaintiffs allege that the companies knowingly made illicit payments similar to those executed during the Oil-for-Food program after the Mahdi's Army had seized control of the Iraqi Health Ministry in 2004. As support for this claim, the plaintiffs cited media coverage of the Mahdi's Army's control of that Ministry during the class period and the Mahdi's Army's use of those funds to operate against the United States Military.

This action is currently in its preliminary stages, with the defendants having recently filed motions to dismiss.

CHAPTER 3: U.K. ANTI-BRIBERY DEVELOPMENTS

I. Overview

On April 8, 2010, the House of Commons passed legislation to consolidate, clarify and strengthen UK anti-bribery law. The Bribery Act 2010 ("Bribery Act") creates four categories of offenses: (i) offenses of bribing another person; (ii) offenses related to being bribed; (iii) bribery of foreign public officials; and (iv) failure of a commercial organization to prevent bribery. The first category of offenses prohibits a person (including a company as a juridical person) from offering, promising, or giving a financial or other advantage: (a) in order to induce a person to improperly perform a relevant function or duty; (b) to reward a person for such improper activity; or (c) where the person knows or believes that the acceptance of the advantage is itself an improper performance of a function or duty. The second category of offenses prohibits requesting, agreeing to receive, or accepting such an advantage in exchange for performing a relevant function or activity improperly.

The third category of offenses, bribery of foreign public officials, is the most similar to the FCPA. According to the Bribery Act's Explanatory Notes, Parliament intended for the prohibitions on foreign bribery to closely follow the requirements of the OECD Convention, to which the United Kingdom is a signatory. Under the Bribery Act, a person (including a company) who offers, promises, or gives any financial or other advantage to a foreign public official, either directly or through a third-party intermediary, commits an offense when the person's intent is to influence the official in his capacity as a foreign public official and the person intends to obtain or retain either business or an advantage in the conduct of business. In certain circumstances, offenses in this category overlap with offenses in the first category (which generally prohibits both foreign and domestic bribery). The MOJ Guidance, however, highlights that the offense of bribery of a foreign public official does not require proof that the bribe was related to the official's improper performance of a relevant function or duty. The overlap between the general bribery offenses and the offenses relating to bribery of foreign officials also allows prosecutors to be flexible, enabling them to bring general charges when a person's status as a foreign official is contested or to seek foreign official bribery charges when an official's duties are unclear.

Finally, and most significantly for large multinational corporations, the Bribery Act creates a separate strict liability corporate offense for failure to prevent bribery, applicable to any corporate body or partnership that conducts part of its business in the United Kingdom. Under this provision, a company is guilty of an offense where an "associated person" commits an offense under either the "offenses of bribing another person" or "bribery of foreign public officials" provisions in order to obtain or retain business or a business advantage for the company. An "associated person" includes any person who performs any services for or on behalf of the company, and may include employees, agents, subsidiaries, and even subcontractors and suppliers to the extent they perform service on behalf of the organization. While failure to prevent bribery is a strict liability offense, an affirmative defense exists where the company can show it had in place "adequate procedures" to prevent bribery.

The offense of failure to prevent bribery stands in contrast to the FCPA's standard for establishing liability for the actions of third parties, such as commercial agents. Whereas the FCPA's anti-bribery provisions require knowledge or a firm belief of the agent's conduct in order for liability to attach, the Bribery Act provides for strict liability for commercial organizations for the acts of a third party, with an express defense where the company has preexisting adequate procedures to prevent bribery. This strict

liability criminal offense creates significant new hazards for corporations when they utilize commercial agents or other third parties. In effect, the actions of the third party will be attributable to the corporation, regardless of whether any corporate officer or employee had knowledge of the third party's actions. The affirmative defense places a great premium on having an effective compliance program, including, but not limited to, due diligence procedures. In the United States, the existence of an effective compliance program is not a defense to an FCPA charge, though the DOJ and SEC do treat it as one of many factors to consider in determining whether to bring charges against the company, and the U.S. Sentencing Guidelines include it as a mitigating factor at sentencing.

The Bribery Act has several other notable differences from the FCPA, and in many ways, the UK law appears broader. Portions of the Act are applicable to any entity that carries on a business, or part of a business, in the United Kingdom, whether or not the underlying conduct has any substantive connection to the United Kingdom. As the then-SFO Director Richard Alderman explained in a June 23, 2010, speech:

> I shall have jurisdiction in respect of corruption committed by those corporates anywhere in the world even if the corruption is not taking place through the business presence of the corporate in this jurisdiction. What this means is this. Assume a foreign corporate with a number of outlets here. Assume that quite separately that foreign corporate is involved in corruption in a third country. We have jurisdiction over that corruption.

Furthermore, the Bribery Act criminalizes bribery of private persons and companies in addition to bribery of foreign public officials. The Act also provides no exception for facilitation or "grease" payments, nor does it provide any exception for legitimate promotional expenses, although it is arguable that properly structured promotional expenses would not be considered as intended to induce a person to act improperly and therefore would not violate the Act.

II. U.K. Legal Privilege in Investigations: Back to Status Quo

On May 8, 2017, Justice Andrews of the High Court of Justice, Queen's Bench Division, handed down a decision in *Serious Fraud Office v. Eurasian Natural Resources Corporation* presenting a restrictive interpretation of both forms of legal privilege in the U.K., litigation privilege and legal advice privilege, as applied to documents created during an internal investigation. On September 5, 2018, however, Eurasian Natural Resources Corporation ("ENRC") prevailed in its appeal of this decision with the Court of Appeal, which largely restored a more expansive understanding of legal privilege as applied to internal investigations.

The dispute originated as part of the SFO's criminal investigation into alleged fraud, bribery, and corruption by ENRC. In August 2011, ENRC engaged outside counsel to conduct an internal investigation into a whistleblower's allegations of corruption in ENRC's wholly-owned Kazakh subsidiary. It later directed the law firm to conduct a second investigation, this time into allegations of impropriety surrounding ENRC's acquisition of a mine in Africa. The investigations, which ran until April 2013, occurred simultaneously with a dialogue between ENRC and the SFO regarding the various allegations.

That dialogue broke down—and the SFO commenced a formal criminal investigation—when ENRC dismissed the law firm conducting the internal investigations and liaising with the SFO on ENRC's behalf.

During the course of its investigation, the SFO sought to compel ENRC to produce documents primarily generated by outside counsel and forensic accountants during the course of the internal investigation. The documents included, among other things, notes taken by outside counsel during investigative interviews. ENRC refused to produce the documents, claiming they were protected by legal advice privilege, litigation privilege, or both. The SFO then brought the matter before the court. Justice Andrews sided with the SFO and, with the exception of slides prepared by ENRC's counsel for presentation to the Board of Directors, determined that the documents were not protected by legal privilege.

With respect to litigation privilege, Justice Andrews held that simply anticipating a criminal investigation by the SFO fails to fulfill the requirement that adversarial litigation be reasonably in contemplation, stating that "prosecution only becomes a real prospect once it is discovered that there is some truth in the accusations, or at the very least that there is some material to support the allegations." Further, litigation privilege only holds if the documents were produced predominantly for the purpose of conducting adversarial litigation. In this case, the court found, the documents at issue were produced first as part of a fact-finding mission, and then in connection with advice about how to reach a civil settlement—in other words, to avoid litigation, rather than to conduct it.

Concerning legal advice privilege, Justice Andrews held that the only documents falling under the umbrella of protection were a set of slides prepared by ENRC's counsel for presentation to the Board of Directors on the Board's request for legal advice. The court found no evidence that the remaining documents summarized legal advice for individuals authorized by ENRC to seek it. Further, it held that the underlying communications were not privileged, because they were not made for the purpose of instructing counsel on behalf of the company. Justice Andrews specifically rejected the contention that a document can be privileged simply by virtue of being drafted by an attorney: "A document . . . that would not be privileged if it had been created by a non-lawyer does not acquire a privileged status just because a lawyer has created it."

In a decision that has been widely applauded by the legal community, the Court of Appeal overturned much of the High Court's decision, largely restoring legal privilege protection to internal investigations conducted by counsel. With regards to litigation privilege, the Court of Appeal held that anticipating a criminal investigation fulfills the requirement that adversarial litigation is reasonably in contemplation. The Court of Appeal held that the lower court was wrong to find that there is a general principle that litigation privilege does not attach in the context of internal investigations until either a company knows the full details of what is likely to be unearthed by the investigation or a decision to prosecute has been made. The Court of Appeal also found that the evidence demonstrated that the documents at issue were created for the dominant purpose of resisting the contemplated criminal proceedings, and that it was of no issue that ENRC considered sharing materials from its investigation with the SFO as part of its negotiation strategy.

Although the Court of Appeal largely agreed with the High Court on legal advice privilege, finding that under current English law the privilege only covers information received by counsel from ENRC or personnel authorized to seek or receive legal advice, the Court of Appeal noted that it would favor a more

expansive interpretation that would include lawyers' communications with employees of the client that were not directly authorized to seek or receive legal advice.

III. Recent U.K. Investigations and Enforcement Actions of Note

1. Guralp Systems Ltd.

On August 17, 2018, the SFO announced an investigation into Guralp System Ltd. for allegedly engaging in corrupt actions in connection with the sale of seismic equipment to the Korea Institute of Geoscience and Mineral Resources ("KIGAM"). Guralp's founder, Cansun Guralp, and an employee, Andrew Bell, were also arrested and charged with conspiracy to make corrupt payments. On September 28, 2018, Heather Pearce, Guralp's former sales director, was similarly charged with conspiracy to bribe a foreign official. In 2017, KIGAM's former director was sentenced to 14 months in federal prison in the United States for using a Southern California bank account to launder bribes that he received from two unnamed seismological companies (see "Heon Cheol Chi," p. 41).

2. Liberty Media (Formula 1)

In its August 9, 2017, Form 10-Q filing and its March 1, 2018, 10-K filing with the SEC, Liberty Media, the ultimate owner of Formula 1, announced its understanding that the SFO was conducting a "pre-investigation" in connection to potential issues related to a 2013 Concorde Implementation Agreement made between Formula 1 and the governing body of world motorsport, the Federation Internationale de l'Automobile ("FIA"). According to media reports, UK Member of Parliament Damian Collins, chairman of the Culture, Media, and Sport Select Committee, asked the SFO to investigate a $5 million payment that the Formula 1 rights holder had made to the FIA, questioning why Formula 1 would need to pay such a large sum to its regulator.

The Director of the SFO confirmed in a May 3, 2017 letter to MP Collins that the SFO planned to investigate the matter.

Meanwhile, FIA issued a statement confirming that the $5 million payment had been made, though it denied any wrongdoing. It explained that the 2013 agreement "introduced a new governance structure for Formula 1 and redefined certain conditions applicable to their relationship, in particular to ensure that the FIA be properly remunerated for its regulatory role."

At the time of the allegedly improper payment, the private equity firm CVC Capital Partners ("CVC") owned a controlling share of Delta Topco, Formula 1's immediate parent company. Liberty Media announced its agreement to purchase Delta Topco from CVC and other sellers on September 7, 2016, and the sale was completed on January 23, 2017.

3. British American Tobacco

On August 1, 2017, the SFO announced that it had opened an investigation into suspected corruption by British American Tobacco ("BAT"), the world's largest publicly traded tobacco company. In November 2015, Paul Hopkins, a former BAT employee who worked for the company in Kenya for 13 years, blew the whistle on BAT's alleged bribery in Africa. In an interview with the BBC, Hopkins characterized himself as a "commercial hitman" who paid bribes on behalf of BAT in order to secure

market share and counter anti-smoking legislation. He also provided emails naming some of the alleged bribery recipients. Among those fingered in the emails were three representatives to the World Health Organization's Framework Convention on Tobacco Control ("FCTC"): Godefroid Kamwenubusa, an official in Burundi's Ministry of Health, Chaibou Bedja Abdou from the Comoros, an official for the Framework Convention on Tobacco Control ("FCTC") (both of whom allegedly received $3,000 each), and Bonaventure Nzeyimana of Rwanda, who allegedly took $20,000. BAT has allegedly described these payments as "unlawful bribes" in internal documents and employment tribunal cases involving dismissals of BAT employees. Former BAT lobbyist Solomon Muyita also alleges that he followed BAT orders and made payments to fifty individuals in Uganda, including seven MPs, including $20,000 to MP Baltazar Kasirivu-Atwooki and David Bahati in 2012 in order to alter a parliamentary report and influence the drafting of new tobacco control laws. Furthermore, Mr. Hopkins has alleged that he made payments to Kenyan officials, including one to Martha Karua for KES 7 million in order to obtain confidential documents of a rival from the Kenyan Revenue Authority, and another payment to Moses Wetangula, including a business class ticket to London so that no paper trail would exist.

In its February 25, 2016, Preliminary Announcement to its shareholders, BAT acknowledged allegations of misconduct in Africa and announced that it had hired an outside law firm to investigate. The internal investigation was ongoing as as of October 2018, and BAT has said that it intends to cooperate with the SFO's investigation.

4. Rio Tinto

On July 24, 2017, the SFO announced that it had opened an investigation into suspected corruption by the Rio Tinto group ("Rio Tinto") related to its activities in the Republic of Guinea. Rio Tinto disclosed on November 9, 2016 that it had notified U.K. and U.S. authorities of the discovery of email correspondence from 2011 concerning $10.5 million in potentially improper payments relating to the Simandou project in Guinea. Rio Tinto indicated that it also planned to notify authorities in Australia. In late 2017, the SFO raided Mr. de Combret's London residence…

According to Rio Tinto, the Simandou project is an "integrated mining and infrastructure development" comprising an iron ore mine, a 650-kilometer train line connecting the mine to a deep-water port, and associated support structures such as access roads and power systems. Under former President Lansana Conte, the government of Guinea originally granted Rio Tinto the Simandou mining concession in the 1990s. However, before President Conte's death in 2008, the government stripped Rio Tinto of half its rights, granting them instead to Israeli-French billionaire Beny Steinmetz's BSG Resources ("BSGR")—a transaction that was itself the subject of an FCPA investigation in the United States. After Guinea elected President Conde in 2010, he accused BSGR of corruption and revoked its rights to develop the mine. Rio Tinto subsequently re-secured full rights to Simandou from President Conde's government in 2011.

Detailed allegations of bribery by Rio Tinto in its efforts to re-secure the rights to Simandou began to appear in the press on November 9, 2016—the same day as Rio Tinto's public disclosure. *Mediapart* published emails from 2011 between Rio Tinto's former Energy & Minerals chief executive Alan Davies, who was then responsible for the Simandou project, a former Managing Director and former Head of Minerals. In those emails, Mr. Davies attempted to justify Mr. de Combret's large fee by citing Mr. de Combret's "unique and unreplicable services and closeness to the President."

In its November 9, 2016 press release, Rio Tinto announced that it had suspended Mr. Davies, who also serves as a non-executive director at Rolls-Royce. Rio Tinto also announced that it had launched an internal investigation led by outside counsel, and that it intended to fully cooperate with any inquiries by authorities.

5. Tesco Stores Limited and Related Individuals

On April 10, 2017, the SFO announced that it had entered into a Deferred Prosecution Agreement with British retail giant Tesco Stores Ltd. ("Tesco"). This announcement, marking the SFO's fourth use of a DPA, followed the SFO's March 28, 2017, statement that the parties had reached an agreement in principle to enter into a DPA under which Tesco would pay a financial penalty of £129 million and reimburse the SFO's investigation costs. In its announcement, the SFO clarified that the DPA related only to the potential criminal liability of Tesco and covered neither the potential liability of Tesco's parent company, Tesco PLC, nor the potential lability of any employee or agent of either company. Details of the final DPA remain unavailable: three Tesco PLC executives are standing trial for apparently related accusations, and the High Court imposed reporting restrictions on Tesco's DPA and the connected factual background until the conclusion of that trial.

The SFO announced on September 9, 2016, that it had charged those three Tesco PLC executives—Carl Rogberg, Christopher Bush, and John Scouler—with one count of Fraud by Abuse of Position and one count of False Accounting. Press reports indicate that all defendants pleaded not guilty to the charges. The charges are based on accusations that the defendants withheld information from auditors and outright falsified electronic accounting records. Due to medical reasons, Rogberg has been removed from the indictment, and Bush and Scouler are scheduled to stand trial beginning on October 1, 2018. If convicted of fraud, each defendant faces up to 10 years in prison. A conviction for false accounting could carry with it a sentence of up to seven years.

The SFO first announced that it had launched a criminal investigation into accounting practices at Tesco PLC on October 30, 2014. The investigation stemmed from Tesco's September 2014 admission that it had overstated that year's first-half profits by £250 million. The U.K.'s Groceries Code Adjudicator also found that the company had deliberately and repeatedly withheld money owed to suppliers in order to artificially boost its sales performance.

6. Rolls Royce

On January 17, 2017, the SFO announced that it had entered into a Deferred Prosecution Agreement with Rolls-Royce PLC ("Rolls Royce") following a four-year investigation. This constituted the third use of a DPA since the tool became available to UK prosecutors on February 24, 2014, under the Crime and Courts Act 2013 (*see* Hughes Hubbard FCPA & Anti-Bribery Compendium, "Rolls Royce").

7. Airbus Group

Airbus reported in its First Half-Year 2017 Financial Report that, in "the context of review and enhancement of its internal compliance improvement programme, [it] discovered misstatements and omissions relating to information provided in respect of third-party consultants" in its applications for export credit financing. Airbus reported that it informed the UK, French, and German export credit

agencies ("ECAs") in early 2016 "of the irregularities discovered," and that it made a similar disclosure to the SFO.

In August 2016, the SFO announced that it had "opened a criminal investigation the prior month concerning allegations of fraud, bribery and corruption in the civil aviation business of Airbus Group." The SFO stated that the allegations related to "irregularities concerning third-party consultants." In a release on March 15, 2017, Airbus announced that France's Parquet national financier ("PNF") had opened a preliminary investigation into the same subject and that the SFO and PNF would act in coordination.

Airbus has stated that it "is cooperating fully with both authorities" on the investigation, and that it has also been "working with relevant ECAs" to address the issues and re-establish export credit financing.

On 22 May 2017, Airbus announced that it had established an independent compliance review panel composed of three members, former German finance minister Theo Waigel, former French European affairs minister Noëlle Lenoir, and U.K. lawyer and House of Lords member David Gold. Airbus CEO Tom Enders stated that the panel "will support us in our ongoing efforts to put in place a meaningful change programme which addresses the issues that have been identified."

CHAPTER 4: ANTI-CORRUPTION ENFORCEMENT UPDATES IN SELECT COUNTRIES

For a number of years, observers could be forgiven for concluding that anti-corruption enforcement was primarily an American activity, and that the FCPA enforcement was the primary—if not only—anti-corruption risk faced by companies. The world is different today.

Below we explore anti-corruption enforcement developments in Brazil, China, France, and Norway.

I. Brazil

A. Introduction

Since the beginning of "Operation Car Wash," Brazil has maintained its position as a major player in the global fight against corruption. The U.S. DOJ and SEC reportedly have dozens of open investigations with connections to Brazil, including probes into Brazilian companies across various industries (*e.g.*, food, power/energy, oil and gas, steel, air transport, telecommunications, banking) and foreign companies operating in Brazil. Moreover, Brazil continues to cooperate in cross-border corruption investigations, including with enforcement colleagues in the U.S., France, Switzerland, U.K., Singapore, and elsewhere.

Brazil's political atmosphere has had a significant impact on its fight against corruption. Conversely, one could say that the fight against corruption has had a significant impact on Brazil's political atmosphere. Eleven of the 13 candidates running for the Presidential office in October 2018 have run campaigns focused on a strong commitment to fight corruption. This suggests that the attention and focus to the anti-corruption campaign is likely to continue for the foreseeable future.

The Clean Record Law[46] has also taken on a larger role in Brazil's political and anti-corruption arenas. The Clean Record Law bars candidates from certain public offices for convictions for any number of specific crimes, including corruption-related offenses. Although eight years have passed since the Clean Record Law was adopted, the increase in anti-corruption enforcement has recently led to an increase in the applicability off the Clean Record Law. For example, the Supreme Electoral Court barred former president Mr. Luis Inácio Lula's attempt to run in the 2018 General elections due to the Clear Record Law.

Below we highlight the most relevant efforts by Brazilian enforcement authorities over the past year. In addition, we examine Brazil's anti-corruption framework and new guidance issued by the Anti-Corruption Unit of the Federal Prosecutor's Office, which provides rules on the negotiation and implementation of corporate settlements under the Clean Companies Act.

46. Enacted as Complementary Law 135, on June 4, 2010.

B. Enforcement Highlights

1. Operation Car Wash

Operation Car Wash is the largest anti-corruption campaign in Brazil's history. It started in 2014 as a small-scale probe into illegal currency exchange and money laundering. Its scope rapidly expanded over the years as Brazilian authorities uncovered evidence of a massive bribery scheme involving Petrobras and other state-controlled companies. According to Brazilian prosecutors, the largest EPCI groups in Brazil colluded to rig bids and fix prices, paying kickbacks to public officials who not only failed to halt the cartel, but also actively favored its members.

As of August 2018, the escalated enforcement efforts from Operation Car Wash included: (i) over 2,400 investigations and enforcement actions against companies and individuals related to allegations of bribery, money laundering, and conspiracy; (ii) over 200 arrests; (iii) over 180 settlements (including leniency agreements with companies and plea bargains with individuals); and (iv) over 500 international cooperation proceedings (including active and passive requests).[47] Brazilian authorities are reportedly seeking to recover a total of BRL 38.1 billion ($12 billion), including fines, as well as funds misappropriated from Petrobras through procurement fraud, inflated prices, and unjustified contract amendments. A significant part of the investigation is confidential; therefore, the probe is likely to produce further developments in the near future.

Individuals investigated and arrested in connection with Operation Car Wash include high-level company executives, commercial agents, Petrobras officials, and Brazilian politicians, including federal congressional representatives, senators, and state ministers. Over the past two years, some of Brazil's most prominent political figures have been charged and convicted of corruption in the scope of Operation Car Wash. In March 2017, Eduardo Cunha, the former speaker of the House, was sentenced to over 15 years in prison on charges that included bribery and money laundering in connection with a Petrobras project in Benin. Cunha is currently in custody and has reportedly engaged in plea bargain negotiations with the Federal Prosecutor's Office.

In connection with his plea negotiations, Cunha reportedly pledged to implicate President Michel Temer in the corruption scheme. In May 2017, reports surfaced that Temer was secretly recorded discussing hush money payments to Cunha with an executive of meatpacking conglomerate JBS. JBS presented the tapes in connection with settlement negotiations.

In June 2017, Brazil's Prosecutor-General presented charges against Temer for corruption for allegedly receiving bribes through an agent to influence a decision by Brazil's antitrust agency (CADE). However, under Brazilian law, the House of Representatives must authorize the indictment of a sitting president. Thus far, Temer has been able to stall formal prosecution with the help of his coalition in Congress. In August 2017, a majority of the House of Representatives voted not to authorize the indictment, thus suspending the charges until Temer leaves office. Prosecutors submitted a second complaint against Temer in September 2017 on the counts of obstruction of justice and conspiracy in the

47. *See* www.mpf.mp.br/para-o-cidadao/caso-lava-jato/atuacao-na-1a-instancia/parana/resultado (access on September 27, 2018, at 03:07 PM).

scope of Operation Car Wash. The House of Representatives have also voted to not authorize his indictment for the second complaint.

In July 2017, Lula da Silva (Brazilian President from 2003-2011) was convicted of corruption and money laundering for allegedly receiving bribes from EPCI giant OAS in order to influence the award of certain Petrobras contracts. He was sentenced to nearly 10 years in prison by the lower court. The Federal Court of Appeals for the Fourth Circuit increased his sentence to nearly 12 years, and he has been in custody since April 2018.

In September 2017, Dilma Roussef (President from 2011 to her impeachment in 2016), Lula, and other members of the labor party ("PT") were charged with engaging in organized crime. The charges stem from claims of widespread corruption during both presidents' administrations. The investigators estimate that certain PT leaders and the party itself collectively received approximately BRL 1.5 billion ($480 million) in bribes between 2002 and 2016. Roussef is currently running for Senator in the State of Minas Gerais, as her impeachment did not result in her debarment from submitting her candidacy for political offices.

2. Operation Skala

Operation Skala is the result of Brazilian Federal Police's efforts to investigate a scheme involving Brazilian President, Mr. Michel Temer. Operation Skala began in March 2018 and aimed to collect evidence related to the supposed favoring of companies in connection with a Decree signed by Mr. Temer directed to the port sector. Operation Skala focused, in particular, on the extension of concession contracts in Santos' port and whether a company called Rodrimar paid bribes to President Temer and his allies. Operation Skala was aided by testimony of Joesley Batista—former chairman of JBS S.A. and a key individual in a separate high profile operation into the meat packing industry—Operation Weak Meat.

Operation Skala is ongoing and has been extended already four times.

C. Anti-Corruption Laws

Since 2013, Brazil has completely overhauled its anti-corruption framework with the enactment of the Clean Companies Act ("CCA") (Law No. 12846/13). Under the CCA, companies are subject to a strict liability standard for bribery and fraud against domestic and foreign public institutions, risking harsh punishment regardless of corrupt intent. Notably, potential sanctions may include monetary fines, debarment from public procurement, and even compulsory dissolution of the business. Since the enactment of the CCA, other regulations have been enacted with an aim to clarify and facilitate the implementation of its requirements.

1. Decree No. 8420/2015

Although the CCA became effective in January 2014, in practice, enforcement was not enabled until over a year later, when then-incumbent president Dilma Rousseff issued a decree regulating key aspects of the law (Decree No. 8420 from March 2015). Among other things, the decree provided sentencing guidelines with a clear focus on prevention, specifically rewarding companies with a strong compliance program in place. To be considered effective and warrant a lesser fine, such a program must include the following elements: (i) an adequate tone at the top; (ii) written integrity policies (*e.g.*,

standards of conduct, code of ethics, anti-corruption procedures) applicable to all employees, members of management and, as appropriate, third parties; (iii) periodic compliance training; (iv) periodic risk assessments, with an aim to enhance and update the compliance program; (v) thorough and truthful bookkeeping; (vi) internal controls ensuring the accuracy of financial reports; (vii) specific procedures to prevent fraud and other misconduct in connection with public tenders, government contracts, and any interactions with public officials (*e.g.,* paying taxes, handling inspections, or applying for licenses), including through third parties; (viii) a compliance function with adequate structure, independence, and powers to implement the integrity program; (ix) adequately publicized reporting mechanisms, which must be accessible to employees and third parties, as well as whistleblower protection measures; (x) disciplinary measures for misconduct; (xi) mechanisms ensuring detection, prompt discontinuation, and timely remediation of misconduct; (xii) due diligence for third parties (including suppliers, contractors, agents, and business partners); (xiii) due diligence, background checks and exposure assessments prior to any corporate reorganization (including mergers and acquisitions); (xiv) continuous monitoring of the compliance program, with an aim to improve internal controls; (xv) transparency in donations to candidates and political parties. In addition to an effective compliance program, other mitigating factors include cooperating with the authorities, self-reporting misconduct, and remediating damages. On the other hand, larger fines are due where management has knowledge of the wrongdoing and fails to prevent it, or where there is a pattern of continuous or recurrent offenses.

Furthermore, the decree also clarified the role of different agencies with overlapping powers to enforce the CCA. Civil sanctions must be pursued in court, through legal action initiated, as a rule, by the Office of the Prosecutor. As for administrative penalties, generally, the government institution directly affected by an alleged offense has primary jurisdiction to conduct and judge the corresponding sanctions proceeding. However, where the primary entity is unwilling or unable to do so, or where multiple federal entities are affected, the Ministry of Transparency and Federal Comptroller-General (“CGU”) has subsidiary jurisdiction over the matter.

2. Regulations by the Ministry of Transparency and Federal; Comptroller-General

In light of its new responsibilities, in April 2015, the Ministry of Transparency and CGU issued additional regulations to structure and govern its sanctions proceedings. Most notably, Regulation No. 909 established a three-prong test for companies to earn a fine reduction based on the implementation of an effective compliance program. Investigated companies must: (i) demonstrate which of the controls described above (as listed in the March 2015 decree) are included in the compliance program, and prove that they are adequate to the company’s size, operations, and relevance in the market; (ii) demonstrate that the program has been consistently and effectively implemented over time, including through written records, statistics, and sample case files; and (iii) demonstrate that the program had been created prior to the alleged misconduct, and prove that the controls were used to prevent, detect, and remediate the specific acts under review. To satisfy such prongs, companies may submit evidence including official documents, emails, memoranda, minutes of meeting, reports, internal policies, and payment or accounting data.

3. New Guidance on Corporate Settlements

Among other innovations, the CCA created the anti-corruption leniency agreement, a specific type of settlement available for implicated companies that choose to cooperate. The law detailed the requirements and benefits of such settlements, but failed to provide sufficient guidance on the negotiation process. This caused uncertainty among different agencies with anti-corruption responsibilities, arguably hampering enforcement.

Over the past year, several agencies have taken steps to address this gap and better define their respective roles on each case. Namely: (i) the CGU and the Office of the Federal Attorney-General ("AGU"); (ii) the Office of the Federal Prosecutor ("MPF"); and (iii) the Federal Court of Accounts ("TCU"), which has powers to enforce certain administrative sanctions and also audit and suspend (where applicable) government acts involving federal entities or funds.

In May 2018, CGU implemented Normative Instruction N. 2/2018, which provides the methodology to calculate administrative fines under the CCA. The disclosed goal was to expand the transparency and consistency of the application of fines. In August 2018, CGU amended Ordinance 910/2015, which dealt with the administrative proceedings established on the CCA. The amendment changed the timing for when investigated companies have to submit their Compliance Program for analysis and to request reduction of fines.

In September 2018, CGU released its new Guidance for Evaluation of Compliance Program under the administrative proceeding established at the CCA. The Guidance provides the requirements and methodology for the analysis and evaluation of a compliance program. This guidance aims to serve as reference for the companies regarding the requirements to be considered when a compliance program is analyzed.

CGU's current Minister, Wagner de Campos Rosário, has been in the office since June 2017. The continuity of Mr. Rosário as Minister for more than one year helped CGU act more consistently when dealing with anti-corruption matters. Prior to Mr. Rosario, former Minister Torquato Jardim occupied the office for less than one year and Mr. Fabiano Silveira and Mr. Luiz Navarro held the position for less than four months combined.

While the precise role of each agency might continue to evolve with practice, these developments suggest that the authorities will increasingly join efforts to negotiate leniency agreements.[48] As of September 2018, seventeen leniency agreements have been entered in Brazil (thirteen with the MPF and four with CGU/AGU).

II. China

2018 marks the start of President Xi's second term and the sixth year of China's anti-corruption campaign. During the first half of the year, Chinese officials kept up their prosecution of corrupt officials

48. With the enactment of Law N. 13,506, of November 13, 2017, Brazilian Central Bank and the Securities and Exchange Commission of Brazil (CVM) are now also able to enter into corporate settlements similar to the leniency agreement provided in the CCA. While the Brazilian Central Bank has already regulated the application of the new legislation through its Regulation 3,857/2017, CVM is still preparing its own regulation on the matter.

and established a new government agency, the National Supervision Commission, with broad powers to audit, inspect, and discipline misbehaving officials. To date, Chinese authorities have received more than 1.68 million complaints and whistleblowing letters, opened 302,000 cases, and punished more than 240,000 officials for violations of the Communist Party of China's ("CPC" or the "Party") disciplinary regulations. The majority of these instances involved corruption and so-called "lifestyle" issues. Over 4,000 officials, for example, were disciplined for "receiving or providing gifts in violation of Party regulations." Notably, since March 2018, monthly reports from the Central Commission for Discipline Inspection of Communist Party ("CCDI") have also included a new category of disciplinary violation—"accepting meals from private parties in violation of Party regulations"—signaling increased monitoring of Party members' ties to private entities.

A. Catching "Tigers" and "Flies"

In his January 2018 meeting with the CCDI, President Xi reiterated his zero-tolerance stance towards corruption and reminded the CCDI that they should uncover and punish violations of Party discipline not only by lower ranking offenders (*flies*), but also against high ranking officials (*tigers*). He also pressed the CCDI to take further measures to address both the symptoms and root causes of corruption to secure a "sweeping victory" against corrupt practices.

Consistent with President Xi's message, the CCDI (working together with the National Supervision Commission) and law enforcement bodies in China, have continued to target corrupt officials of different levels. In the first six months of 2018, 14 officials above the ministerial level were prosecuted and at least ten other "tigers" were placed under investigation. For example, Sun Zhengcai, a former Party Politburo member who was once believed to be one of China's next generation of leaders, was sentenced to life in prison on May 8, 2018 for accepting RMB170 million (approximately $25 million) in bribes. In the same month, former Deputy Minister of the Ministry of Finance, Zhang Shaochun, and former Vice Governor of Guizhou Province, Pu Bo, were placed under investigation for "severe violations of regulations and Party discipline." Prosecutions of lower level officials similarly escalated in 2018. Among the 240,000 officials disciplined in the first half of 2018, over 190,000 officials (80%) were below township level. Based on data from the CCDI, approximately 60% of the officials involved in "corruption and lifestyle issues that directly affect the people" are village representatives. The CCDI has stated publicly that it believes that corruption at this level greatly hinders China's poverty alleviation work, and that because China has vowed to lift all of its citizens above the poverty line by 2020, rooting out this low level corruption has become a major part of China's poverty relief plan. The CCDI also indicated earlier this year that the fight against corruption and malpractice in poverty relief initiatives is a major task for the following three years, and harsh punishments will be imposed on corrupt officials implicated in misuse of poverty relief funds.

B. Supervision Law and the National Supervision Commission

On March 20, 2018, China adopted the Supervision Law, which replaced the Administrative Supervision Law from 1997 and established the National Supervision Commission ("NSC"), the supreme agency for combating misconduct. The NSC is tasked with monitoring and investigating misconduct by "public power holders" in China, including looking into misconduct such as corruption and bribery, abuse of power, dereliction of duty, tunneling of interests, favoritism, and squandering of state assets. Unlike the 1997 Administrative Supervision Law, which only focused on public servants, the Supervision Law

empowers the NSC to monitor, investigate, and discipline anyone who is considered a "public power holder," which includes persons who serve in the Chinese government, anyone subject to the PRC Civil Servants Law, employees of organizations authorized to administer public affairs, managerial personnel of SOEs, managerial personnel of public institutions in the education, scientific research, cultural, healthcare, and sports fields, and others who perform public duties. The Supervision Law also established supervision commissions ("SCs") at the subnational levels, including provinces, autonomous regions, counties, cities, and districts of cities.

Integrated Anti-Corruption Regime—The formation of the NSC is meant to create a more efficient anti-corruption enforcement regime in China. Prior to the creation of the NSC, anti-corruption tasks were divided among different actors with overlapping functions: the CCDI supervised Party members and enforced Party discipline; the Ministry of Supervision monitored duty-related misconduct by public servants according to the 1997 Administrative Supervision Law; the Anti-Corruption Bureau and Anti-Malfeasance Bureau within the Supreme People's Procuratorate ("SPP") were responsible for investigating and prosecuting crimes related to corruption and malfeasance, and the National Bureau of Corruption Prevention was primarily responsible for international anti-corruption coordination and assistance. With the establishment of NSC, all of the supervisory, corruption prevention, and control departments mentioned above, aside from the CCDI, are now integrated into the NSC, creating a more streamlined system. The NSC and the CCDI will work together and share resources and personnel. Yang Xiaodu, former Deputy Secretary of CCDI, has been elevated to oversee both agencies.

Greater Jurisdiction—The NSC is empowered to supervise anyone who holds public power, regardless of that person's political association or official title, which creates a broader scope of jurisdiction than was previously available. For example, in the old system, individuals who were not Party members or public servants but who participated in public functions (*e.g.* contractors hired by a local government) were rarely supervised. Under this expanded jurisdiction, the number of people who are supervised under by the anti-corruption regime increased significantly.

Consolidated Powers—The NSC, along with the supervisory commissions at lower levels, has the authority to collect evidence, seize assets, question witnesses, detain suspects, conduct searches and seizures of individuals or entities, and recommend cases for prosecution. Some have expressed concerns that the NSC's powers are too broad. For example, the Supervision Law grants supervision commissions at various levels the power to detain a suspect at a select location if certain conditions are met, such as when the suspect is likely to run away, commit suicide, or destroy evidence. In such situations, the suspect can be detained for up to six months without the right to counsel. Nevertheless, this is considered an improvement from the old "shuanggui" mechanism, by which Party members could be detained without an official charge for years. The Supervision Law also added procedural requirements to prevent potential abuse of powers. The family of the detained will be notified within 24 hours and the detained will be provided proper access to food, rest, and, if needed, medical care.

International business entities operating in China do not literally fall under the purview of the Supervision Law or the jurisdiction of the NSC. Nevertheless, the Supervision Law and the NSC have the potential to impact international companies operating in China as well as their employees. For instance, Supervision Law allows the NSC to detain private individuals deemed to have bribed public power holders.

C. Focus on Active Bribery

During the CPC's 19th National Congress in October 2017, President Xi reiterated that those who pay bribes, as well as those who receive bribes, will face punishment. While China has historically been more tolerant of active bribery as opposed to passive bribery, an increasing number of investigations have focused on active bribery. According to the SPP's 2018 Work Report, in the past five years, more than 37,000 bribe-givers were prosecuted, an 87% increase compared to the five-year period before. A recent article in the newspaper run by the CCDI-NSC indicated that both active and passive bribery must be rooted out together to help the Party deter corruption. The article also called for more investigations against bribe-givers by CCDI-NSC branches of difference levels.

This focus is also evident at the provincial level. In May 2018, the CCDI-SC of Jiangsu Province passed a work plan that focuses on active bribery. A local official commented that the establishment of supervision commission provides an opportunity to allow Jiangsu to use cases against officials who accept bribes to prosecute the bribe payers. The manager of the Jiangsu CCDI-SC similarly indicated that those who pay bribes will be severely punished, and that any improper benefits obtained through bribery will be confiscated. Jiangsu also plans to adopt a blacklist of individuals and companies that are caught paying bribes. This blacklist will lay the foundation for the CCDI-SC of Jiangsu and other government agencies such as the industry and commerce administration to build an integrity system, which would largely prohibit bribe payers from participating in any type of business activities.

D. The Party's Inspections of State-Owned and Affiliated Entities

Similar to previous years, the CPC continues to dispatch teams to conduct inspections of state-owned and affiliated entities and institutions. In 2018, the first round of inspections started in February and covered Party organizations in 14 provinces, eight central government agencies including the Ministry of Commerce and the State Food and Drug Administration, and eight state owned entities.

The main purpose of these inspections is to test the reviewed entities' compliance with the Party's integrity and anti-corruption principles. In 2018, the inspection teams extended the review period of each target from two months to three months. During the onsite visits, the inspection teams reviewed documents, collected whistleblowing letters and complaints, and interviewed relevant employees. The inspection teams released their findings in July 2018. Among other things, the teams found frequent violations involving improper hiring and promotion, employees living beyond their means, and issues involving procurement and bidding activities. The inspections also found that concerns identified in prior inspections had not yet been fully addressed. The inspections teams recommended that the local CCDI-NSCs monitor the status of the improvement on these issues and hold relevant officials accountable if the issues are not properly resolved.

E. International Manhunts and International Cooperation

In July 2014, China launched "Operation Fox Hunt," a campaign aimed at repatriating fugitives and recovering stolen assets. In March 2015, building on the success of Operation Fox Hunt, Chinese authorities announced the launch of a broader anti-corruption campaign code-named "Operation Sky Net." Operation Sky Net not only focuses its efforts on the repatriation of economic crimes fugitives and the recovery of stolen assets, it also aims to prevent corrupt officials and assets from leaving the country

in the first place. Among other things, Operation Sky Net has been cracking down on illegal personal IDs and passports and investigating underground banks and offshore companies used for transferring illicit assets.

A number of government agencies and departments are involved in Operation Sky Net, the most important of which include the People's Bank of China, the Party's Organizational Department, the SPP, and the Ministry of Public Security. Each agency leads an operation with a particular focus. For example, the People's Bank of China is responsible for collaborating with various commercial banks to monitor and prevent money laundering and the transfer of illicit assets, and the SPP focuses on combating abuse-of-power crimes and retrieving stolen assets from abroad.

Shortly after the launch of Operation Sky Net, the CCDI, in cooperation with the Chinese Central Bureau of the International Criminal Police Organization ("Interpol"), released a "100 most wanted" list of Chinese fugitives. The list includes the suspects' photos, identification numbers, visa numbers, crimes reportedly committed, and possible countries of hiding. Among the 100 fugitives, 40 were believed to have fled to the U.S.

By the end of April 2018, through Operations Fox Hunt and Sky Net, China has recovered RMB 10 billion (approximately $1.45 billion) and repatriated 4,141 fugitives from more than 90 countries and regions. Fifty-two fugitives on the most wanted list have been returned to China.

China's cooperation with law enforcement authorities from a number of countries has led directly to these achievements. Historically, many Western countries have been reluctant to enter into extradition treaties with China due to continued allegations and reports of mistreatment of criminal suspects and lack of due process. However, beginning with Spain in 2006, China has successfully ratified treaties with several European countries, including France, Portugal, and Italy. Even in countries with which China has no extradition treaties, China has been actively seeking more mechanisms for cooperation. In November 2017, China and member states of the Association of Southeast Asian Nations ("ASEAN") released a joint statement on strengthening anti-corruption cooperation, which includes closer cooperation and assistance between law enforcement bodies. In January 2018, at the meeting with the Community of Latin American and Caribbean States ("CELAC"), China and the member states formed an Action Plan for 2019 – 2021. The Action Plan includes the reinforcement of legal assistance and cooperation through information exchange in the areas related to money laundering, asset recovery, and extradition.

F. China's New Anti-Unfair Competition Law

China's Anti-Unfair Competition Law ("AUCL") regulates various forms of unfair practices, including commercial bribery. On November 4, 2017, China adopted amendments to the old AUCL. The current AUCL became effective on January 1, 2018.

Compared to the old AUCL, the current AUCL reflects a number of changes on key issues. This includes protection of trade secrets, internet-related unfair competition, powers of the administrative enforcement authorities, and commercial bribery. Some key anti-corruption features in the current AUCL are outlined below.

Bribes to third parties are prohibited. While the 1993 AUCL only prohibited bribery between the parties to a transaction, the current AUCL includes third parties as well. Article 7 of the current AUCL states that business operators must not use money or property or any other means to bribe a party to a transaction or any *third party* that might affect the transaction. "Third party" is broadly defined by the current AUCL as any entity or individual with authority to influence the transaction.

Vicarious liability for the employer. The 1993 AUCL did not include vicarious liability for a company for the acts of its employees. This has allowed some companies to willfully ignore employees' conduct and use employees as scapegoats for misconduct that had benefited the company. The current AUCL creates a rebuttable presumption that a company is liable for the corrupt conduct of its employees except when it can demonstrate that the employees violated the employer's interests through their corrupt conduct. This means companies in China are liable for the acts of their employees by default, placing a heavier burden on companies to adopt effective compliance systems and to train and exercise controls over employees' actions.

Fines and penalties. For commercial bribery, the 1993 AUCL imposed a fine ranging from RMB10,000 to RMB200,000 (approximately from $1,500 to $30,000), as well as confiscation of illegal income resulting from the bribery. In the current AUCL, the range of the monetary fines has been raised to RMB100,000 to RMB3,000,000 (approximately $14,000 to $437,000). The current AUCL has also included revocation of business license as a penalty in serious offences.

G. Corporate Compliance

In December 2017, China's first National Compliance Management System Guideline ("Compliance Guideline") was approved and released by the General Administration of Quality Supervision, Inspection and Quarantine and Standardization Administration.

The Compliance Guideline, which became effective on August 1, 2018, was developed based on ISO 19600 standards on compliance management. As the first national compliance standards, the Compliance Guideline offers a framework for companies to establish, implement, evaluate, and improve their compliance systems.

As the range of the anti-corruption campaign continues to expand, Chinese regulators have placed more weight on corporate compliance. As part of a pilot program that began in 2016, the State-owned Assets Supervision and Administration Commission of the State Council have encouraged key SOEs including China Petroleum and China Mobile to adopt compliance programs that meet the requirements of the Compliance Guideline. The compliance systems within these key SOEs will serve as examples for other SOEs going forward.

More recently, the China Council for the Promotion of International Trade, a state-backed trade council, stated that compliance risk has become one of the core risks for Chinese firms in the international market. On July 5, 2018, China's National Development and Reform Commission released a draft version of its own guidelines, called the International Operations Compliance Management Guideline, for public comment. These guidelines address the structure of compliance programs, risk assessments, compliance implementation, and compliance culture cultivation. The guidelines refer to the Compliance Guideline but with a focus on international operations.

Similar to ISO 19600 standards, both the Compliance Guideline and International Compliance Guideline are broad but provide great flexibility. While the effect of these compliance guidelines remains to be seen, they provide a good foundation for Chinese companies that wish to establish compliance programs consistent with international best practices.

III. France

As with many OECD signatories, France has faced criticism regarding its lack of enforcement of foreign corruption cases. It has taken these critiques to heart and, in 2016, instituted sweeping changes to its anti-corruption legal framework in order to force companies to develop and maintain corporate compliance programs that can prevent and detect corrupt practices. France has also passed laws that seek to impose other ethical practices on French companies. The following section will examine France's evolution in the anti-corruption landscape, how these practices affect companies working in France, and how the anti-corruption landscape is likely to develop.

A. Sapin II

Under international pressure to comply and implement its obligations under the OECD Convention on Combating Bribery of Foreign Officials in International Business Transactions ("OECD Convention"), France enacted a series of reforms targeting corrupt activities and promoting transparency. The most significant of these to date is Act No. 2016-1691, entitled "Transparency, the Fight against Corruption and the Modernization of the Economy" (named after then Minister of Finance, Michel Sapin, hereinafter "Sapin II"). As part of these reforms, France: (i) criminalized the influence peddling of foreign officials; (ii) extended French jurisdiction over certain corruption related offenses; (iii) created a version of a deferred prosecution agreement ("DPA"); (iv) created the *Agence Française Anticorruption* (French Anticorruption Agency, or "AFA"); (v) required companies of a certain size to adopt and implement anti-corruption compliance programs; (vi) introduced a new criminal penalty through the court-imposed monitorship; (vii) provided additional protections for whistleblowers; and (viii) imposed an obligation to disclose links of interests on lobbyists.

1. Criminalization of the Influence Peddling of Foreign Officials

Prior to the passage of Sapin II, "influence peddling" (*trafic d'influence*) – or the use of one's influence in government or connections with persons vested with authority in order to obtain undue favors or treatment – was punished only if carried out on domestic, French officials, or on officials of a public international organization (such as the United Nations). Under Sapin II, the offenses of active and passive influence peddling have been extended to include foreign government officials. Persons found guilty of influence peddling face penalties of up to five years imprisonment and a maximum criminal fine of 500,000 euro or double the proceeds of the offense (whichever is the greater), bearing in mind that criminal fines against companies can be multiplied by up to five times those against natural persons (which would amount to penalties of up to 2.5 million euro).

2. Extension of French Jurisdiction Regarding Corruption Offenses

Sapin II extended the extraterritorial reach of French anti-corruption law in two significant ways. First, it removed certain requirements that previously limited French prosecutors in foreign corruption

cases. Under French law, criminal offenses that occur abroad are typically subject to a "dual criminality" requirement. In other words, to be punishable in France, the conduct must represent a criminal offense under the laws of France and the country where it occurred. Sapin II removed this requirement for acts of corruption and influence peddling, meaning that such acts can be prosecuted in France regardless of whether they represent a criminal offense abroad.

Sapin II also extended application of French criminal laws regarding corruption and influence peddling to any defendant that conducts part or all of its business in France. Under Sapin II, corruption and influence peddling laws will be applicable in any instance where the defendant is a French national, ordinarily resides in France, or conducts part or all of its business in France.

Another consequence of Sapin II is that the French public prosecutor no longer has a monopoly on initiating prosecution or actions against a company for alleged bribery of a foreign public official. Potential victims of the offense are allowed to trigger prosecution by filing a complaint with the investigative magistrate. This expansion of the law is already being tested in practice, with certain civil society organizations (such as Transparency International France and Sherpa) bringing civil claims for alleged corrupt conduct.

Such expansion of the French prosecutors' extraterritorial reach in corruption cases may allow French prosecutors to take a more active role in enforcing foreign bribery violations, which in turn may increase the number of prosecutions of corruption of foreign officials. If such an increase was meant to address the OECD's recommendations, the parliamentary debates showed that it was also aimed at aligning the scope of French anti-corruption laws with those of other jurisdictions, such as the U.S. Foreign Corrupt Practices Act and the U.K. Bribery Act.

3. Creation of a French DPA—La Convention Judiciaire d'Intérêt Public

Implemented as part of Sapin II, the "judicial settlement of public interest" (*Convention judiciaire d'intérêt public* or "CJIP") is considered to be a major breakthrough in contemporary French anti-corruption law and provides French prosecuting authorities with tools more aligned with their foreign counterparts. It was also one of the most debated elements of Sapin II. The primary criticisms were that such a mechanism favors a financial transaction over the defense of the public interest, that it prevents public debate and excludes the victim from the settlement, and that it is reserved for companies and not applicable to individuals. After having been abandoned from the draft bill, the CJIP was reintroduced and reshaped to address certain aspects of these criticisms. Eventually adopted, the CJIP, which was inspired by deferred prosecution agreements ("DPAs") already used in the U.S. and U.K., is aimed at aligning France with these foreign counterparts and allowing faster and more efficient resolutions for companies.

The CJIP provides corporations (even those below the financial and personnel thresholds set for the implementation of a compliance program) with the possibility to settle certain criminal cases outside of the courtroom. This alternative resolution mechanism is available only for companies and not for individuals. Hence, the potential benefits of the CJIP do not extend to the companies' representatives and employees, who remain subject to prosecutions even though such a settlement agreement is entered into by the legal entity. However, the *Parquet National Financier* publicly stated that the plea agreement

procedure (*comparution sur reconnaissance préalable de culpabilité* or "CRPC") could be available for individuals who agree to the alleged facts.

The CJIP is to be offered at the initiative of the public prosecutor or the investigative judge, depending on the stage of the prosecution. The public prosecutor (not the AFA) may propose a settlement agreement to an implicated company as long as the company has not been formally charged ("[*t*]*ant que l'action publique n'a pas été mise en movement*") with the offence eligible for that type of resolution. Alternatively, when the case has been brought to the investigative magistrate (*juge d'instruction*)—which means that the public prosecution has already been initiated—the latter can decide to transmit the case to the public prosecutor with the view to offer a CJIP to the company which has been put under investigation (*mise en examen*).

The CJIP is available only in cases that could be characterized as offences of corruption, influence peddling, and/or laundering of the proceeds of tax fraud and related offences. The CJIP instrument must fulfill a number of formal requirements. It contains a precise statement of facts and their legal characterization but requires no admission of guilt. In addition to these requirements, the company that has been put under investigation needs to acknowledge the alleged facts and agree to their proposed legal characterization. In any case, the CJIP shall include the following obligations: (i) the payment of a public interest fine that is to be proportionate to the gains made from the breach, without exceeding 30% of the entity's average annual turnover on the last three years; (ii) the implementation of a compliance program under the supervision of the AFA for a maximum of three years; and, (iii) the indemnification of any known victim, with payment having to be made within a year.

Fundamentally, the Sapin II CJIP agreement must be subject to judicial scrutiny, with the prosecutor proposing the draft settlement to the court. A public hearing is held, following which the judge decides whether or not to approve the settlement, verifying the appropriateness of the procedure, the legality of execution, the amount of the fine, and the proportionality of the terms in light of the benefits derived from the violations. The decision cannot be appealed. If the court approves the settlement, the company has ten days to withdraw its acceptance. The approval order has no finding of guilt and has neither the nature nor the effect of a conviction. The CJIP settlement, the approval order, and the amount of the fine are to be published on the AFA's website.

If the court does not approve the settlement, or if the company withdraws its acceptance/does not satisfy the terms of the agreement, the prosecutor then moves forward with the prosecution. If the court does not approve the settlement or the company withdraws its acceptance, then the prosecutor cannot mention statements made or documents provided by the company in the course of settlement discussions before an investigative magistrate or at trial. In contrast, the law does not guarantee confidentiality in the situation where the prosecution resumes because the company failed to comply with the requirements imposed by the CJIP.

It is possible that a sanction agreed under a CJIP—of up to 30% of the entity average annual turnover—could be greater than the sanction set forth by the Penal Code. In March 2017, the attempted CJIP offered to UBS for settling a case of tax fraud was refused by the bank which considered the proposed fine, 1.1 billion euro, to be excessive. Since then, five companies have agreed on paying the fine provided for in the CJIP rather than taking the risk of being tried in court. In the absence of formal directions in the law as to how to conclude or implement a CJIP, the outcomes of these five CJIPs

combined with the circular issued by the Ministry of Justice on January 31, 2018 provide some insight on the following main aspects.

First, while Sapin II's wording implies that the decision to enter into negotiations for the purpose of agreeing to a CJIP lies only with the prosecutor, it appears that, in practice, such an option might also be suggested by the implicated company. Indeed, in all the approving court orders, the judge noted that the CJIP resulted from the company's counsel's "clear and unequivocal" request to enter into negotiations with the prosecutor. Notwithstanding such option, the decision to enter into negotiations ultimately rests with the prosecutor who, according to the circular issued by the Ministry of Justice on January 31, 2018, shall make his decision depending on whether the company: (i) spontaneously reported the facts at issue; (ii) cooperated in the context of the investigation; and, (iii) already entered into such agreement in the past (which would most likely lead to the exclusion of a new CJIP).

Second, while Sapin II's provisions indicating that the public interest fine is to be established *in proportion* to the ill-gotten gains suggest: (i) the amount of the improper advantage is the only reference value to take into account; and (ii) only a portion of such advantages will be included within the public interest fine component, the precedents to date show that it is not the case. Not only is the entirety of the ill-gotten gains at issue systematically used as a basis of calculation, it is also balanced by other considerations which appear to play as mitigating or aggravating factors. This is in line with the circular issued by the Ministry of Justice on January 31, 2018, pursuant to which the prosecutors are recommended to: (i) first calculate the entire amount of the improper advantage—which shall cumulate both direct and indirect profits gained because of the corruption scheme; and then (ii) apply a multiplying or mitigating coefficient. According to the Ministry of Justice, the multiplying coefficient shall be equal to at least two, be applied depending on the gravity and the duration of the faulty behavior, and based on the case history of the legal person at fault. In addition or alternatively to the aggravating factor, the Ministry of Justice invites the prosecutor to apply a mitigating factor where they deem that the facts at issue are particularly old, whenever the company self-reported them, cooperated during the proceedings, took remediation actions and/or implemented preventive measures. As described in greater detail below, the five CJIPs concluded so far offer a good illustration of what enters into consideration regarding the calculation of the public interest fine. They all used the entire amount of ill-gotten gains as a basis and applied an "additional penalty," the amount of which was more or less consequential depending on the aggravating and/or mitigating factors.

More details on each CJIP are provided below.

- *HSBC Private Bank (Suisse) SA*: On October 30, 2017, the Swiss bank HSBC PRBA entered into a CJIP with the French financial prosecutor and, as such, gave rise to the first-ever corporate resolution. In its CJIP, HSBC agreed to pay a 157,975,422 euro public interest fine (86,400,000 euro as a restitution of profits and 71,575,422 euro as a penalty) and 142,024,578 euro in damages, in order to resolve a four-year criminal investigation into the bank's assistance in helping French clients conceal their assets from the French tax administration.

  HSBC was indicted for: (i) unlawful banking and financial solicitation of prospective French clients committed by unauthorized persons; and (ii) laundering the proceeds of tax evasion,

with the latter offense being explicitly eligible for the CJIP and the former offense being considered "connected" to the latter.

The entire amount of the ill-gotten gains was included in the public interest fine, and additional financial penalties were also imposed based on the seriousness of the facts and the duration of the faulty behavior. The settlement refers to the fact that the bank "neither voluntarily disclosed the facts to the French criminal authorities, nor acknowledged its criminal liability during the course of the investigation" and "only offered minimal cooperation in the investigation." However, the HSBC CJIP also noted that from the time the investigation was launched until December 2016 when Sapin II came into force, the French legal system did not provide for a legal mechanism that encouraged full cooperation. While it is also the case for the other CJIPs, the HSBC CJIP is the only one to contain such a statement. At the time of the HSBC CJIP, the January 2018 Ministry of Justice's circular had not been issued. Since then, the abovementioned circular confirmed that self-disclosure was to be taken into account as a criterion to offer the company at fault the opportunity to conclude a CJIP and as a mitigating factor in the calculation of the public interest fine. Here, and as opposed to the other CJIPs concluded so far, the total amount of the fine corresponds to the maximum public interest fine allowed under Sapin II *(*30% of the company's average gross annual turnover over the last three years).

The fact that the CJIP did not require HSBC to implement an effective compliance program under the supervision of the AFA likely results from the fact that this CJIP was concluded for offenses related to the laundering of tax evasion profits, activities which neither fall within the primary competence of the AFA nor are the primary focus of Sapin II-required compliance programs. Following the court's approval of the CJIP on November 14, 2017, the criminal prosecution against HSBC was formally terminated on November 28, 2017 when the bank complied with the requirement to pay 300 million euro within a ten-day period. This illustrates one notable difference between the CJIP and the DPA in the United States. Whereas DPAs in the United States systematically defer prosecutions for a certain period of time pending satisfactory conclusion of whatever terms the DPA sets forth, proceedings in France against a company entering into a CJIP are formally terminated on the date of which its obligations are met, irrespective of the potential immediateness of such obligations.

- In 2018, French prosecutors entered into three CJIPs involving a corruption scheme within the procurement department of EDF (Électricité de France, a French electric utility company largely owned by the French State). All three companies were involved in active public corruption for having yielded to the requests of EDF's procurement officer in order to obtain and maintain maintenance contracts. The prosecutor took into account, as aggravating factors, the duration of the faulty behavior, and the fact that the offense had been made within the framework of a contractual relationship with an operator responsible for a public service mission. Although the amount of the public interest fine varied for each case, depending on the gravity of the misconduct and the amount of the profits illegally obtained from the misconduct, the damages awarded to EDF was invariably 30,000 euro for each of the defendants. These CJIPs concluded with the French prosecutor in Nanterre, confirming that corruption-related prosecutions do not fall within the exclusive competence of the French National Prosecutor.

- *SAS SET Environnement*: On February 14, 2018, the French company SAS SET Environnement entered into a CJIP with the French prosecutor, agreeing to pay a public interest fine of 800,000 euro (680,000 euro as a restitution of profits and 120,000 euro as an additional penalty, to be paid in four installments) and 30,000 euro in damages. In addition, SAS SET Environnement committed to implementing and complying with an effective compliance program under the supervision of the AFA for two years (with such supervision-related costs capped at 200,000 euro). SAS SET Environnement is a small company, with 125 employees and turnover of between 10 and 20 million euro over the past eight years. This case is an example of how companies which do not meet the thresholds provided by Article 17 of Sapin II (companies with at least 500 employees and a turnover of over 100 million euro, or companies that are part of a group with a total of at least 500 employees and a consolidated turnover above 100 million euro) may nonetheless be compelled to implement a compliance program in line with the legal requirements of Article 17. Here again, the entire amount of the profit illegally gained was included in the public interest fine. In order to assess the amount of the additional penalty, the judge took into account the abovementioned aggravating factors and highlighted, as mitigating factors, the fact that: (i) the President of the company involved in the offense left the company and sold his shares; (ii) the General Secretary and the Chief Financial Officer involved in the offense were terminated; and, (iii) new shareholders and a new management team not involved in the offense are now in place. The CJIP was approved by the court on February 23, 2018.

- *SAS Kaefer Wanner*: On February 15, 2018, the French company SAS Kaefer Wanner (subsidiary of the German group Kaefer) entered into a CJIP with the French prosecutor, agreeing to pay a public interest fine of 2,710,000 euro (in twelve installments) and 30,000 euro in damages. They additionally agreed to submit to the AFA's control for 18 months in order that the AFA can assess the company's compliance program currently in place and make recommendations (with such supervision-related costs capped at 290,000 euro). It is interesting to note that the French authority will be monitoring the French subsidiary of a foreign entity, which may be one of the first steps towards the international spread of a French-style compliance program. In order to assess the fine, the above-mentioned aggravating factors were taken into account. However, the prosecutor also noted a number of mitigating factors, including the fact that the company cooperated with the investigation and took measures to detect and prevent corruption. The CJIP highlighted that SAS Kaefer Wanner changed its management and governance rules, provided anti-corruption training to its employees and strengthened its ethics program. All these measures led to a fine which ended up being lower than the amount of the ill-gotten gains (the illegal profits were estimated to 3.3 million euro whereas the fine was set to 2.71 million euro). This is the only case so far where the mitigating factors weighted more than the aggravating ones in the assessment of the fine. The court's decision approving this CJIP has not been published on the AFA's website.

- *SAS Poujaud*: On May 4, 2018, the French company SAS Poujaud (subsidiary of the French group Altrad) entered into a CJIP with the French prosecutor, agreeing to pay a public interest fine of 420,000 euro (240,000 euro as a restitution of profits and 180,000 euro as an additional penalty, to be paid in two installments) and 30,000 euro in damages. The company was additionally required to submit to a compliance program under AFA's supervision during two years (with such supervision-related costs capped at 276,000 euro). All the illegal estimated profits were included in the fine and increased by the abovementioned aggravating factors. With regards to the mitigating factors, the prosecutor noted that the fact that SAS Poujaud neither spontaneously revealed the facts, nor cooperated during the proceedings, deprived the company of a mitigating factor in that respect. In other words, although SAS Poujaud did not benefit from mitigation based on these elements, these factors were not used to worsen the assessment of the faulty behavior by the prosecutor and to increase the amount of the fine. The CJIP nevertheless noted two mitigating factors: (i) the implementation of an Ethics Code; and (ii) the fact that the directors left the company. The CJIP was approved by the court on May 25, 2018.

- *Société Générale SA*: On May 24, 2018, the French company Société Générale SA entered into a CJIP with the French financial prosecutor. By doing so, it agreed to pay a public interest fine of 250,150,755 euro (*i.e,* 167,437,431 euro as a restitution of profits and 82,713,324 euro as an additional penalty) and agreed to have its compliance policy assessed by the AFA over the course of two years in order to resolve an investigation on active corruption of foreign public agents involving a Libyan intermediary. Société Générale SA was criticized for having financed, through the payment of non-standard commissions, luxury trips and gifts to the benefit of the Libyan Investment Authority's (LIA) executive director in exchange of numerous investments made by LIA to Société Générale SA.

  The U.S. Department of Justice (DOJ) started investigating these acts in 2014, and the French financial prosecutor cooperated with the DOJ when it started its own investigation in 2016 by coordinating their investigations and sharing evidence. They eventually decided to split the total amount of the fine (500,301,511 euro) in half. The totality of the ill-gotten gains was part of the fine, plus an additional penalty to take into account the exceptional gravity of the facts, the duration of the corrupt behavior and the fact that they involved foreign public officials. The CJIP noted that the damages due to the victim (963 million euro had already been paid by Société Générale SA within the framework of civil proceedings carried out in front of the High Court of Justice of England and Wales; therefore, there was no need to indemnify LIA as part of the CJIP. The Société Générale CJIP is not only the first one to be concluded on the basis of corruption of foreign public officials, but also the first to be concluded in the course of a preliminary investigation. As such, the company did not have to adhere to the legal characterization of the facts, but only to their existence, as opposed to the four other CJIPs where the signing company had been indicted and thus required to adhere to these two elements.

The CJIP mentioned the fact that Société Générale SA improved its compliance and anti-corruption policy and has continued to develop such policies and procedures. The company will be under monitorship for two years, during which the AFA will assess the quality and effectiveness of its compliance policy and will provide recommendations. The expenses linked to such monitorship shall be paid by the company up to a threshold of 3 million euro, which is 10 to 15 times greater than the expense cap set out in the other three CJIPs. The CJIP was approved by the court on June 4, 2018.

4. Creation of a New Anti-Corruption Agency: AFA

As noted above, Sapin II created the AFA, the authority primarily responsible for preventing and detecting acts of corruption and influence peddling in both the public and private sectors. The AFA has policy-making authority and enforcement powers limited to administrative sanctions, although it may refer cases to the prosecutor's office for criminal action if the AFA uncovers possible criminal activity while performing its mission. Its head is appointed by the President of the French Republic for a non-renewable six year term, reports to both the Ministers in charge of Justice and the Budget (*Ministre de la Justice* and *Ministre du Budget*). As of writing this, the current head is Charles Duchaine, a former prosecutor, who was appointed in March 2017.

Sapin II further provided that the AFA may issue tailored recommendations that will be regularly revised in light of practices in order to assist corporations in preventing and detecting acts of corruption. It may also initiate independent reviews to control the quality and the effectiveness of corporate compliance programs, including by requesting documents and carrying out site-visits, publishing reports, and taking enforcement actions. Enforcement actions include imposing administrative sanctions on companies and individuals for violations of the obligations described above.

The AFA can decide to investigate possible violations of Sapin II compliance obligations (see below) on its own or at the request of, *inter alia*, either the President of the French High Authority for the Transparency of Public Life (*Haute Autorité pour la Transparence de la Vie Publique*) or the French Prime Minister. AFA agents may request documents and conduct onsite interviews, although they must provide notice prior to visiting a company's premises. Following a review, the AFA will issue a report assessing the audited company's compliance with the Sapin II compliance program obligations. Since the AFA is responsible for reviewing compliance with the obligations to prevent and detect corruption and influence peddling described above, it does not have to establish the elements of underlying criminal offenses of corruption and influence peddling in order to sanction companies. In other words, the AFA can sanction a company for not having in place the elements of a compliance program as dictated by Sapin II, whether or not an act of underlying corruption can be established.

Concluding the review, the AFA will have a number of choices. Its President may issue a warning and request that corrective action be taken. Alternatively, it may decide to initiate enforcement proceedings before the AFA's Sanctions Committee. If an enforcement proceeding is held, the company will have the opportunity to present observations, and a hearing will be held. The Sanctions Committee may impose fines on individuals of up to 200,000 euro and a fine of up to one million euro on companies. The Sanctions Committee can also enjoin the company to take appropriate action to adopt an adequate compliance program within a certain period of time (maximum three years). These sanctions can be cumulative, but the amount of the fines shall be proportionate to the seriousness of the infringement and

will take into consideration the financial situation of the person or company in breach. Any decision issued by the AFA's Sanctions Commission ordering an injunction or a financial penalty may be made public and can be appealed before administrative courts. It is important to note that it remains unclear whether such an appeal shall go directly before the *Conseil d'Etat* (the French Supreme Court for public matters) or not.

Another feature under Sapin II is that the AFA may verify, at the request of the Prime Minister, compliance with law 68-678 (the French "Blocking Statute") where a company headquartered in France is subject to a monitorship arising out of settlement with a foreign authority and has to transfer information in that context. Sapin II does not, however, mention that the AFA would carry out similar reviews for Blocking Statute compliance when the foreign settlements involve offenses outside of corruption or influence peddling. The law similarly does not indicate that the AFA should play this role in the context of foreign-led *investigations* (as opposed to completed settlements).

It is important to note that the AFA does not have the authority to investigate bribery, nor does it have to impose criminal penalties, both of which continue to fall under the authority of French prosecutors. Given the recent adoption of Sapin II and these changes, the manner in which the AFA and French prosecutors will collaborate and share information in practice remains to be seen.

5. Creation of an Affirmative Obligation to Implement a Compliance Program

a. Scope

Under Sapin II certain companies are required to implement a compliance program in order to prevent and detect acts of corruption. The compliance program requirement applies to: (i) companies established under French law with at least 500 employees and with a turnover of over 100 million euro; and (ii) companies established under French law that are part of a *group* with a total of at least 500 employees, where the parent company is headquartered in France, and the group has a consolidated turnover above 100 million euro. These obligations also apply to state-owned companies and to the subsidiaries of entities subject to Sapin II requirements.

If a company/legal entity meets the aforementioned criteria, the requirement to implement an adequate compliance program also applies to its president, chief executives (*directeurs généraux*), managing directors (*gérants*) and, under certain circumstances, members of the management board. The French legislature intentionally made the compliance program broadly applicable and placed responsibility on natural persons in an effort to ensure that anti-corruption compliance programs would be implemented through the ranks of French companies.

b. Entities' Compliance Programs

Companies and legal entities falling under the scope of Sapin II are required to implement anti-corruption compliance programs that include the following eight elements:

- a code of conduct defining and illustrating the prohibited conducts likely to constitute an act of corruption or influence peddling ("Code of Conduct");

- a regularly updated assessment of the potential risks of exposure to external corruption ("Risk Assessment");
- internal whistleblowing procedures designed to report violations to the Code of Conduct;
- third-party due diligence and risk-assessment procedures for clients and intermediaries;
- internal or external financial controls ensuring that the company's books and records are not used to conceal acts of corruption or influence peddling;
- training programs for executives and employees potentially exposed to corruption risks;
- disciplinary procedures in case of corruption misconduct by employees; and
- an internal mechanism to evaluate and monitor the effectiveness of the compliance measures.

As noted above, following its control, the AFA makes a report on the company's compliance program and, where necessary, makes recommendations in order to improve it. In cases where entities fail to implement their compliance programs, the AFA, upon completion of its controls, may issue sanctions as described above.

c. AFA's Support Actions

On October 2, 2018, the AFA released its Business Support Charter (*Charte d'appui aux entreprises*), which establishes the framework for the relationship between companies and the business support function of the AFA for the purposes of its mission to help organizations prevent and detect corruption. Since the needs of companies may differ according to their size, sector of activity, economic model, and the sophistication of their compliance system, the AFA has set forth three categories of support.

The first category of support is referred to as generic support, which is intended for all companies concerned with detecting and preventing corruption, regardless of the company's size or sector. Generic support consists of the AFA developing, updating and disseminating the French anti-corruption framework, on the basis of Sapin II's legal requirements. This includes the AFA Recommendations (*see* below), practical guides, responses to general interest questions published on the AFA website, and all other relevant standards for preventing and detecting corruption.

The second category of support is referred to as specific support. It consists of the AFA clarifying or providing expertise on issues raised by a group of companies that have already set up an anticorruption program or are in the process of doing so. The AFA can provide specific support through proofreading documents for the companies or through technical workshops for small groups, which will be organized by sector of activity, job (*i.e.*, compliance officer), or anticorruption issues.

The third category of support provided by the AFA is individual support, which consists of the AFA responding to the specific questions of a specific company. This can be done by mail or email, or through individual coaching at the request of the company for a period not to exceed five months. In the case of

individual coaching, the AFA will guide a company in relation to the implementation or updating of its compliance program, in an effort to ensure that the company understands the applicable anticorruption standards as well as the methods available for deploying a compliance program. AFA's guidance will be based on documents produced by the company and will be discussed during regular meetings between the company and the AFA scheduled jointly by the parties. It does not, however, constitute a certification of the company's compliance program. All companies, regardless of size and sector, can request individual coaching by the AFA, although AFA will evaluate the request and determine whether individual coaching or another form of support would be more appropriate for the particular request. The individual coaching will last as long as agreed between the AFA and the relevant organization (not to exceed five months) unless the organization decides to end the mission before the agreed date or the AFA considers that the company does not respect its commitment to allocate relevant resources to the relevant project. Companies are not obligated to follow the recommendations made by the AFA in the course of the coaching period, and the information shared with the relevant AFA agents is confidential and subject to professional privilege. It is important to note that the support and advisory mission of the AFA remains separate from its enforcement mission, as each function is exercised by a different division of the AFA.

d. AFA's Recommendations on the Compliance Program

On December 21, 2017, the AFA issued specific recommendations concerning some of the required elements of a compliance program under Sapin II, the relevant parts of which are included below:

- **Top Management's Commitment to Preventing and Detecting Corruption**: While it is not part of the legal requirements, the AFA emphasizes in its guidelines that senior management's commitment to a zero-tolerance policy is fundamental for preventing and detecting corruption.

- **Anti-Corruption Code of Conduct**: In addition to the legal requirements set forth in Article 17, II of Sapin II, the AFA recommends *inter alia* that the Code of Conduct be: (i) initiated by the organization's top management; (ii) set out the organization's values and commitments; (iii) describe the internal whistleblowing system offered to employees; (iv) be written in French and translated to be understood by foreign employees; (v) be used as a tool for external communication when dealing with customers, users, suppliers and any other partners of the organizations; and (vi) be regularly updated, especially after any significant update of the risk map (*e.g.,* in the case of a reorganization or restructuring).

- **Internal Whistleblower System**: While Sapin II requires companies to implement an internal whistleblower system allowing employees to disclose conduct or situations that do not comply with the company's Code of Conduct, the AFA made some recommendations in line with the requirements pertaining to the whistleblower procedure as a more general feature of companies' organization, set out by Article 6 and seq. of the Sapin II (*see* below). As such, the AFA encourages entities to implement a single whistleblowing system and, hence, recommends that it specify the information required with respect to the Article 6 whistleblowing system, including the following: (i) the person in charge of receiving whistleblowers' reports; (ii) the measures taken to ensure confidentiality of the

disclosures and the identity of the persons alerting the company and affected by the alert; (iii) the procedures for communicating with the whistleblower and to inform him/her, respectively, of the progress made with processing and handling the alert; and (iv) where appropriate, the policy on processing anonymous reports. The whistleblower protection status may be applied in the framework of this system if conditions presented in greater detail below are met.

- **Risk Mapping**: According to the AFA, the risk mapping must be comprehensive, formalized, and adaptable over time to changing risks. The AFA's guidelines provide a specific methodology to follow consisting of: (i) identifying risks that are inherent in the organizations' activities; (ii) assess the company's exposure to "gross risk" of corruption through the analysis of risk factors or sources (such as high-risk countries, new products, complex contracts, business pressure); (iii) probability of occurrence of the identified risks (for instance, based on a history of incidents); and (iv) existence of aggravating factors (by applying risk coefficients for example); (v) assess the adequacy and effectiveness of mitigating measures in order to determine to what extent they allow computation of the "net" or "residual" risks exposure; (vi) prioritize risks depending on their scores, and (vii) implement an action plan.

- **Third-Party Due Diligence Procedures**: While Sapin II requires companies to conduct due diligence on certain categories of third parties (customers, lead suppliers and agents), the AFA considers that such categories are only "priorities" and recommends that companies review all the third parties with which they have or are about to start a relationship. In addition, the AFA's guidelines provide that due diligence should be conducted before starting any relationship, updated periodically, and proportionate to the risk level. Among the information that the companies are recommended to assess, the AFA includes international sanctions lists. In addition to conducting third-party due diligence, the AFA recommends heightening third parties' awareness by: (i) notifying them of the company's compliance program; (ii) providing them with the company's Code of Conduct and anti-corruption training; and (iii) requiring them to provide a written commitment to combat corruption (anti-corruption clauses should be included in risky contracts) and to check the integrity of their subcontractors.

- **Accounting Control Procedures**: In its guidelines, the AFA states that accounting control procedures have two main goals; first, safeguarding the company's assets and cash resources by checking that operations are well-managed and allocated resources are properly used; and second, ensuring that the company's books and accounts are not used to conceal acts of corruption. Such procedures provide reasonable assurance that a company provides a reliable, regular, sincere, faithful, and complete picture of its accounting and financial situation. Accounting controls can include controls (internal procedures), audits (independent assessments), or both, and can be carried out internally or externally. In any case, the AFA recommends three levels of controls.

- **Corruption Risk Training**: Companies are required to implement "robust [and] appropriately designed" internal anti-corruption training. Such training should particularly be attended by board members, directors, managers, and employees that are most

exposed to corruption risks. Over time, all employees should have been trained to prevent and detect corruption. The training may be delivered internally, by the company itself, or through external consultants, and the company should develop a set of indicators to track the implementation of the training program. While Sapin II only refers to managers and the most exposed employees, the AFA recommends that other employees also be trained, at least on a simplified basis (*i.e.*, fewer topics, not necessarily in-person sessions).

- **Internal Monitoring and Assessment System**: In addition to what is required by Sapin II, the AFA recommends three levels of controls. The first level of controls, performed by operational or support staff, or by line managers, aims to ensure that the all operational or support tasks are carried out in compliance with the company's procedures. The second level of controls, performed by the head of compliance (or other designated manager), is meant to ensure that the first level of controls is properly implemented and that the internal monitoring and assessment system is working properly. The third level of controls, which refers to "internal audits," is intended to ensure that the system to prevent and detect corruption complies with the company's requirements and is efficiently implemented and kept up to date. Based on the risk mapping, the company must develop an audit plan identifying all functions and individuals involved in the monitoring system.

Finally, the AFA's guidelines provide some clarifications for public sector entities (*i.e.,* the State and other administrations linked to the State, local governments, public establishments, public interest groups, publicly owned companies, and non-profits with a public service mission).

While companies already subject to the U.S. FCPA or the U.K. Bribery Act shall already have implemented compliance programs that are compliant with the above-mentioned Sapin II requirements, attention needs to be paid to certain specificities, including the need to follow applicable rules under French Labor Law and Data Privacy Laws. We note that, although the AFA's guidelines are not legally binding, in practice, the AFA generally follows its own recommendations—which are broader than what the law requires—when auditing companies' compliance programs.

e. Medef's Guidelines on the Compliance Program

Following the enactment of Sapin II, the *Mouvement Des Entreprises de France* ("Movement of French Enterprises"), or "MEDEF," published a practical guide on September 22, 2017 regarding the anti-corruption measures implemented by the French anti-corruption law.

The practical guide is not a binding standard for companies and legal entities falling under the scope of Sapin II. However, it provides guidance and gives explanations of the legal requirements to set up effective anti-corruption compliance mechanisms. The guide presents, in the form of summary sheets, practical solutions on how to implement: (i) an assessment of potential compliance risks; (ii) a code of conduct; (iii) due diligence and compliance procedures; (iv) internal or external accounting and financial procedures; (v) compliance training sessions; (vi) whistle-blower procedures; (vii) disciplinary sanctions; and (viii) internal mechanisms to evaluate and monitor the preventive measures in place.

The guide also provides templates of third-party due diligence questionnaires as well as the ICC rules on combatting corruption.

f. The AFA's Audits

The AFA's activities to date have shown it to be effective and ambitious in fulfilling its mission to prevent corruption and related offenses. The AFA contemplates implementing control measures in approximately fifty private sector entities per year (we note that, to date, 1,570 private sector entities may be subject to the AFA's controls) to ensure compliance with Sapin II's requirements. However, and as stated above, the first audits, notified in October 2017 to six companies, as well as the following ones launched in February 2018, show that not only does the AFA asses compliance with the legal requirements as set out in Article 17 of Sapin II but also compliance with its own recommendations—which, as explained above, appear broader than what is stated in the letter of the law.

As partly presented in the "Charter of Rights and Duties of Parties under Audit" issued by the AFA in October 2017 and experienced in real controls, the process can be divided into the following eight steps:

- **Audit Notice**. The AFA sends an audit notice to the representative of the audited company by way of a letter with acknowledgment of receipt. This notice both informs the company of the identity of the agents in charge of the control, and requires the company to answer a general questionnaire of 163 questions inquiring not only about the compliance program but more generally about the company's activities, organization, etc. After the first wave of controls, this questionnaire (slightly revised) was made available on the AFA's website.

- **Communication of Documents and Answering the AFA Questionnaire**. The audited company has 15 days to submit its answers to the aforementioned questionnaire and communicate supporting documents as well as those requested by the AFA through the questionnaire. Since the questionnaire has been made available, companies wisely have begun to start gathering information on an anticipatory basis in order to be able to provide required responses easily and without freezing the organization in case of a control.

- **Discussions with the AFA**. A preliminary courtesy meeting may be organized between the AFA's agents and the audited company.

- **Document Review ("*contrôle sur pièce*")**. The AFA undertakes its review of the documentation provided. This usually gives rise to followup questions from the AFA to the audited company. The last controls show that such questions can take the form a new questionnaire.

- **Onsite Audit Notice**. Fifteen days before the onsite audit, a notice is sent to inform the audited company of the dates on which the agents will come onsite and the identity of individuals that the audit team will interview. It is worth noting here that the interviewee regularly (if not systematically) can include external stakeholders. In 2017, the average number of interviews conducted by the AFA in this context was 21. The latest controls show that the number of interviews can be significantly higher.

- **Onsite Audit**. The AFA reviews documentation and conducts interviews in the audited company's premises.

- **Additional Discussions and Exchanges**. The audited entity may have further exchanges with the AFA after the onsite audit ends, although no new document communicated after such deadline will be taken into account by the AFA.

- **Audit Report**. The AFA eventually prepares a report discussing the audit process and assessing the quality of the anti-corruption program in place within the entity, with a specific emphasis on "tone at the top." The report is divided into "Observations," "Recommendations," and "Finding of Breach." In fact, the law explicitly provides that following its control, the AFA makes a report on the company's compliance program and, where necessary, recommends improvements.

- **Observations of the Audited Company on the Audit Report.** The audited company has two months to comment on the AFA's findings and to challenge, as the case may be, their merits.

- **Issue of the Final Report.** The AFA issues the report in its final version, replying, as the case may be, on the company's comments and arguments.

Our experience shows that, so far, none of the audited companies were spared the finding of a breach. However, as of the date of publication of this Alert, to the best of our knowledge no decision has be made to send one of them before the Sanction Commission.

6. Creation of a Court-Imposed Monitorship

Another novelty of Sapin II is that judges may resort to a new penalty in corruption and influence peddling cases. Courts can sentence companies found guilty of corruption or influence peddling to a form of remediation by requiring them to submit themselves to a compliance program under the supervision—though not necessarily the conduct—of the AFA for a maximum duration of five years. That requirement may also be included as part of the CJIP tool described above for a maximum duration of three years. We note that a monitorship was included in all corruption-related CJIP so far, with a duration set to 18 months or two years. In both instances, the AFA reports to the prosecutor at least annually on the implementation of the program. The AFA will also be able to rely on the help of "experts" or "qualified authorities," suggesting that the arrangement may bear similarities to corporate monitorships as used in the U.S. and other jurisdictions to assist regulators in determining whether a corporate defendant is meeting its obligations deriving from a settlement agreement or court order. Nonetheless, to be similar to monitors used by U.S. authorities, such experts would have to be chosen by the company and approved by the prosecution authorities, which does not seem to be the case under French Law. Indeed, the AFA recently launched call for tenders in order to assist its agents in the conduct of monitorships. To our knowledge, the companies at stake were not involved in the selection process, which confirms that they do not have their word in the choice of the entity who will be in charge of assessing the effectiveness of its compliance program. In any case, any cost incurred by the supervision of the AFA and the assistance of such experts are to be assumed by the convicted legal person, although such costs shall not exceed the amount of the fine incurred for the offense of which the subject was found guilty.

7. Reinforced Protection for Whistleblowers

Despite a strong cultural preference against denunciating, French law introduced incremental protections and rules for whistleblowers. While the protection system progressively introduced by law was disseminated throughout various statues and limited to whistleblowers reporting specific wrongdoings (corruption, public health, conflict of interests, offenses and clear and serious breach of Law), Sapin II enshrined a harmonized and strengthened whistleblower protection regime.

According to the definition set forth by Sapin II, a whistleblower is an individual who discloses or reports, selflessly and in good faith: (i) a crime or a misdemeanor under French Law; (ii) a clear and serious breach of an international commitment duly ratified or approved by France, of an act of an international organization pursuant to such engagement or of French Laws or regulations; or (iii) a serious threat or harm to the public interest, of which he or she has personal knowledge. The French Constitutional Court (*Conseil constitutionnel*) highlighted that this definition was not restricted to employees and external or occasional collaborators of the company targeted by the alert. Despite the fact that this whistleblowing falls out of its mission scope and because the AFA appears to encourage the adoption of a single whistleblowing system, its Recommendations reiterate the five characteristics of a whistleblower, as set forth in Article 6 and seq. of Sapin II: (i) he/she is an individual (not a legal entity); (ii) he/she has personal knowledge of the facts disclosed; (iii) he/she acts selflessly and (iv) in good faith; and (v) he/she discloses serious matters.

It is worth noting that contrary to the US Dodd-Frank whistleblowing provisions, the French whistleblowing system is against any kind of financial incentive being provided for the benefit of the whistleblower. Not only is the whistleblower required to act “selflessly,” but he/she cannot be provided with any financial support. In fact, while the initial version of Sapin II provided that the Defender of Rights (*Défenseur des droits*) could grant, on the whistleblower’s request, financial assistance, such possibility was invalidated by the French Constitutional Court (*Conseil constitutionnel*).

The law provides that a whistleblower must follow a three-step reporting procedure in order to be entitled to protection. First, the whistleblower shall file a report to his or her line manager or employer or a person appointed for this purpose by the employer. In fact, private entities employing more than 50 persons are required to implement internal reporting procedures in order to enable their employees to initiate whistleblower alerts when necessary. Although no penalties are provided for failure to comply with such an obligation, companies must be aware that implementing a reporting system is in their best interests since, absent such system, they minimize the chances to keep a potential alert at the internal level (as opposed to the authorities and/or the public). Second, in the absence of an appropriate action undertaken within a reasonable time, or where there is a serious and imminent danger, the whistleblower may inform French judicial, administrative, or professional authorities. In this respect, the whistleblower may consult the Defender of Rights (*Défenseur des droits*) in order to be directed toward the appropriate authority. Third, and as a last resort in the absence of reaction from such authorities within a three-month period, the whistleblower may alert the public/report to the press.

If the above criteria for whistleblower status are met, then whistleblower status confers a protection under both criminal and labor law. With respect to criminal law, a whistleblower who breached a secret protected by law may benefit from criminal immunity under certain circumstances. With respect to labor law, the whistleblower will be granted a protection within the workplace. This protection makes it

unlawful to exclude from or discriminate a whistleblower in the recruitment process, internships, or professional training, to fire him/her, or to make him/her suffer any disciplinary sanctions as a result of having issued a signal or an alert. Any measure taken in violation of this protection will be null and void.

8. The Creation of an Obligation to Disclose Links of Interests of Lobbyists

Since Sapin II, in France, individuals engaged in lobbying, referred to as "representatives of interests," must be listed in a dedicated National Registry kept by the *Haute Autorité pour la Transparence de la Vie Publique* ("HATVP"—French High Authority of Transparency in Public Life) and to follow ethics rules. Prior to these new provisions, disclosure of lobbying activities was done on an opt-in basis and applied only in the context of contacts made with parliamentarians. The provisions of Sapin II related to lobbyists all entered into force as of July 1, 2018, on which date 1,600 registrants had disclosed their lobbying activities on the National Registry.

Lobbyists are defined under French statute as any natural person, as well as any private or public company, employing persons whose main activity is to influence public decision. This particularly includes influencing the content of laws and regulations by liaising with public officials, including members of the Government, members of the houses of Parliament, and certain local elected officials.

Representatives of interests must disclose to the HATVP the following information:

- For an individual, his/her identify; for a legal person, the identity of its managers as well as its employees entrusted with lobbying activities;
- The scope of his/her/its lobbying activities;
- Acts in lobbying as well as the amount of expenses related to those activities in the previous year;
- The number of persons employed in carrying out its lobbying tasks and, as the case may be, the company's turnover for the previous years;
- Professional or trade union organizations or any association related to the represented interests to which he/her/it belongs.

Failure to comply with these obligations may be punished with a fine of up to 15,000 euro and imprisonment of up to one year. The HATVP has the power to request documents and to conduct onsite verifications upon a judge's authorization, although any of the information collected in the context of its mission shall be treated as confidential.

With its new anti-corruption landscape, there are good reasons to believe that prosecutions as well as convictions based on corruption of foreign officials, will increase. In fact, to date, there is only one decision of conviction for corruption of foreign officials. On February 26, 2016, the Paris Court of Appeals held that Total and Vittol, two French companies, were guilty of corruption of foreign public officials in the context of the United Nations' "Oil-for-Food Program" and imposed fines on each of the companies in the amounts of 750,000 euro and 300,000 euro, respectively. The decision was confirmed in that respect by

the *Cour de Cassation*, France's highest court. Before this case, the *Tribunal de grande instance de Paris* (*Paris Court of First Instance*) found French company Safran guilty of corruption of Nigerian public officials and imposed on the company a 500,000 euro fine. However, on January 7, 2015, the Paris Court of Appeals overturned this decision, and Safran's conviction was overturned.

B. Enforcement Action: the Cour de Cassation's ruling in the Oil for Food Case

On March 14, 2018, five years after the first instance ruling where all defendants were acquitted and 18 months after the informative ruling of the Paris Court of Appeal, the Criminal Section of the *Cour de Cassation* (decision No. 16-82117) issued the latest ruling in the "Oil-for-Food" scandal. Long and complex, this decision notably confirmed the Paris Court of Appeal's decision in that it sentenced some of the defendants for active corruption of foreign public officials. Beyond that, the case is worth some analysis in that its merits may draw consequences on prosecution of corrupt acts in France.

1. Background of the case

Following the invasion of Kuwait by Iraq in early August 1990, the United Nations (UN) established an embargo regime that prohibited the provision of funds or resources to the Iraqi government. However, due to difficulties faced by the Iraqi population, the UN Security Council adopted Resolution No. 986 on April 14, 1995 in order to ease this embargo by allowing Iraq to sell oil, providing that certain conditions were met. These conditions, framing the so-called "Oil-For-Food Program," required the State Organization for the Marketing of Oil ("SOMO"), a state-owned company attached to the Iraqi Ministry of Petroleum, to sell petroleum at a given price set below the oil market price and paid on an escrow account under UN control, which was meant to ensure that the funds were used to acquire food and basic necessities by the State.

However, from 2000 onwards, the Iraqi regime applied a "tax" or "surcharge" on sales worth 10% of the value of a barrel, in violation of UN Resolution No. 986. The companies were required to pay the surcharge by the Iraqi Revolutionary Command Council, holding both executive and legislative powers in the country, if they wanted to pursue their commercial relations with SOMO and continue buying oil in Iraq. While the funds corresponding to the price set by the UN were to be transferred on the escrow account, companies were required to pay the "surcharges" either: (i) into accounts opened in Jordan or Lebanon in the name of SOMO, its officers, or Iraqi officials, or (ii) in cash at various Iraqi embassies. Such transfers were by definition neither controlled nor approved by the UN.

2. The narrow scope of the principle of *ne bis in idem*.

In the first instance, the *Tribunal Correctionnel* notably considered that one of the defendants (Vitol) could not be prosecuted in France, pursuant to Article 14(7) of the 1966 International Covenant on Civil and Political Rights (ICCPR), under a theory of *ne bis in idem*, which prohibits the prosecution or conviction of a person twice for the same act. In fact, in November 2007, this defendant had already entered into a plea deal in the New York State court for the same facts. As for the other defendants, the judges of first instance considered that the components of the offences at stake were not characterized.

With respect to this question, the Court of Appeals considered that while Article 14(7) of the ICCPR may apply to multiple jurisdiction prosecutions, the settlement reached in the US and the charges in France were different. Indeed, defendants were charged in France with "active corruption of foreign public official," while the defendant's guilty plea in the U.S. covered "grand larceny."

The *Cour de Cassation*, after asserting that Article 14(7) of the ICCPR only applies to cases "*whereby the two proceedings have been initiated on the territory of the same State*," considered that the transnational principle of *ne bis in idem* was non-applicable in the present case, although a plea bargain had already been reached by the concerned defendant in the U.S. In line with its longstanding case law, the *Cour de Cassation* held that *ne bis in idem* does not apply in situations where a French court's jurisdiction over the matter is territorial (*compétence territoriale*). In fact, while Article 113-9 of the French Code of Criminal Procedure provides that *"no prosecution may be brought against a person who establishes that he was subject to a final decision abroad for the same offence* (…)," "*in the cases set out under Articles 113-6 and 113-7*," *i.e.*, when the offense was committed as a whole outside French territory, no such limitation is set forth within the law when the offence was committed, even partly, in France. This longstanding principle can be explained by the French courts' attachment to their sovereignty over criminal cases committed on their territory, which will not yield in the face of foreign decisions. This decision is consistent with other recent case law rendered by the same *Cour de Cassation* on January 17, 2018, which involved the CEO of a Gibraltarian company who had bribed Nigerian authorities in the context of a public procurement. However, while a plea agreement had been concluded in the U.S. by the CEO and the U.S. DOJ to put an end to investigations in the country, the *Cour de Cassation* had set aside the settlement. According to the *Cour de Cassation*, the transnational principle of *ne bis in idem* could not apply since part of the facts at stake had been committed partially on the French territory, which thus enabled the executive's prosecution in France.

3. The extensive scope of Article 435-3 of the French Criminal Code with respect to the notion of corrupt person

The *Cour de Cassation* approved the appellate court's reasoning that the surcharges were beneficial to the Iraqi government, noting that no article in the OECD Convention of 1997 excluded a State from being considered as a beneficiary of corruption (even though it also did not explicitly define it as such). Indeed, according to the *Cour de Cassation*, Article 435-3 of the French Criminal Code, as worded at the time of the reproached facts, covered the situation whereby a person yields to unlawful requests "*from agents of a body having the status of a person entrusted with a public service mission,* (…) *conveying requests for payment of hidden commissions made by a State's representative bodies, which are its final beneficiaries*."

Applied to today's wording of Article 435-3 of the Penal Code, which applies to advantages promised to a government official "either for his/her own benefit or that of a third party," the decision of the *Cour de Cassation* can be read to mean that the "third party" under the French Penal Code may be a State.

4. The extensive scope of Article 435-3 of the French Criminal Code with respect to the notion of illicit payments

The defendants argued that the offence of corruption of foreign public officials could not be characterized because Article 435-3 of the French Criminal Code required that offers, promises, donations, gifts, gifts or benefits be requested "without right" (*sans droit*). On the basis of the OECD Convention, which provides that "*it is not an offense if the advantage was permitted or required by the written law or regulation of the foreign public official's country, including case law*," the defendants made the argument that the taxes they were paying to the Iraqi regime resulted from a decision made by the Iraqi Revolutionary Command Council, holding both executive and legislative powers in the country at that time, and circulated through various memoranda to the different Ministries.

The *Cour de Cassation* sided, however, with the Paris Court of Appeal by stating that "it [had] not been established [by the defendants] that the hidden commissions, whose payments were requested by Iraqi State agents outside the scope of the market organized by UN Security Council Resolution No. 986 of April 14 1995, were permitted or required by the written law or regulations of the Iraqi State." By doing so, the *Cour de Cassation* reversed the burden of proof requiring that the defendants prove that such surcharges were permitted by the written laws or regulations of the Iraqi State. This appears to be consistent with the prosecutors' position pursuant to which they are to consider that there is a presumption of lack of right to advantages given or offered to foreign officials. In any case, the *Cour de Cassation* followed the Court of Appeal's reasoning, when it considered that international transactions in Iraq were at the time governed by Resolution No. 986, which forbid such surcharges, as Iraq was a failed State, and could not adopt proper legislation to translate the Resolution into law.

C. Other Related Legislative Initiatives

France has recently adopted other legislative initiatives aimed principally at increasing transparency among businesses to prevent corruption and also to require companies to prevent environmental and human rights violations within their control. These laws include the "Devoir de Vigilance" ("Obligation of Vigilance") and the implementation of the Fourth European Anti-Money Laundering Directive. More generally, France also enacted a law extending the statute of limitation for felonies and misdemeanors.

1. Devoir de Vigilance

Following a lengthy debate first initiated in 2013, the *Devoir de Vigilance* law, passed on February 21, 2017 and approved by the Constitutional Counsel on March 23, 2017, introduces a new principal of a duty of care for companies with respect to their subsidiaries, suppliers, and subcontractors. The bill received strong popular support since it was proposed in response to a series of human rights violations committed by large companies, specifically the 2013 structural failure of Rana Plaza in Bangladesh, in which over 1,000 employees were killed in the collapse of an eight-story commercial building. However, the Senate considered that the bill would place a significant and unique burden on French companies, which would place them at a commercial disadvantage compared to their competitors. Such a law was also considered to be unnecessary since the Directive 2014/95/EU already requires large entities to disclose information regarding their Corporate Social Responsibility policies.

The law applies to French companies that have at least 5,000 employees in France or which employ over 10,000 individuals worldwide. Under the law, companies must create risk mitigation plans (*plans de vigilance*) in order to monitor stages of the supply chain and to prevent risks to the environment, human rights, health, and also corruption. These risk mitigation plans must be implemented for the large companies themselves, but also for their affiliates, subsidiaries, and suppliers, both in France and abroad. Hence, even if it is estimated that only 150 to 200 companies will be directly covered by this law, smaller companies will also be impacted if they are suppliers or subcontractors to companies subject to the law.

The risk mitigation plans shall include: (i) a risk mapping intended to identify, analyze and rank the risks; (ii) due diligence and risk assessment procedures to be conducted on subsidiaries, subcontractors and suppliers; (iii) appropriate actions of risk mitigation and prevention of serious breaches; (iv) a whistleblowing report procedure allowing the collection of relevant information in light of the risks targeted; and, (v) a followup and assessment mechanism of the measures undertaken in response to the risks identified. Given the similarity of the mechanisms and measures required under the Law on the Duty of Care and Sapin II, companies subject to both laws may wish to consider merging their processes to avoid duplication and inconsistencies.

Where a company subject to such requirements has been notified to fulfill its obligations and did not comply within a three-month time limit, it can be ordered to do so and, as the case may be, have a fine imposed (*astreinte*) by the relevant jurisdiction (a priori the Commercial Court) and upon the request of a person able to prove a legal interest. Given the wording of the provision, it remains unclear whether the prior notice is a condition or a mere option to a judicial claim. In addition, any person able to prove its legal interest may file a claim for damages before the competent jurisdiction (a priori the Commercial Court).

The draft bill initially included the possibility to set a civil penalty of up to 10 million euro or 30 million euro in the event of a severe breach of the fundamental rights protected by the Law. However, due to the lack of clarity of the terms used by the legislator for describing the obligations subject to such a fine, the French Constitutional court censored the provisions at issue. In other words, failing companies are not subject to criminal penalties.

2. Anti-Money Laundering

France's arsenal to combat money laundering and terrorist financing ("AML-TF legislation" hereinafter) is based on the general offense of money laundering. The detection of illicit financial flows also relies on due diligence requirements imposed on certain professions and organizations.

On December 1, 2016, France implemented the fourth European Anti-Money Laundering Directive via Ordinance No. 2016-1635. The goal of the law is to strengthen anti-money laundering legislation in France and prevent the financing of terrorism.

a. The expansion of the AML-TF legislation scope

In December 2016, the scope of the entities subject to AML-TF legislation has been broadened to include not only financial service companies, but also non-financial service companies trading fine stones, fine metals, jewels, furniture, interior decorative items, cosmetics, textile products, leather goods, fine

food, clocks, and tableware, accepting payments in cash above an amount set by a 2018 decree at 10,000 euro. In addition, the French Monetary and Financial Code (*Code monétaire et financier*) now specifies that AML-TF requirements embrace both legal and natural persons falling into the listed categories.

The AML-TF requirements are similar to the anti-corruption measures and procedures required by Sapin II, but in respect of anti-money laundering, and include: (i) a risk assessment; (ii) policies adjusted to the risk assessment; (iii) internal controls and procedures set accordingly; (iv) an organization including a person identified as in charge of implementing the AML-TF compliance program who must be sufficiently high in the hierarchy and understand AML risk faced by the company; and (v) adjustments to the recruitment policy. Persons belonging to group of companies, when the mother company is headquartered in France, must set up their AML-TF compliance program at the level of the group (including in their subsidiaries outside France) and share information among group companies.

Subject persons are required to conduct certain verifications on their customers before entering into a business relationship, including verifying their identity and their ultimate beneficial owner. This requirement must also be fulfilled for occasional customers when a red flag arises. When the risk seems low and if the normal business activity otherwise would be interrupted, such verification can be performed during the business relationship instead of before. Various levels of verifications are set by the law depending on the risks. In particular, they must set up internal risk-based mechanisms to identify whether customers are politically exposed persons (PEPs) as defined by French law and perform supplemental verifications on them.

Eventually, in case of infringement of AML-TF legislation by a legal entity subject to it, the applicable sanction might also be imposed on directors, employees and persons acting on behalf of the entity at issue, if they are found to have been personally involved.

In 2017, the French banking authority (*Autorité de Contrôle Prudentiel et de Résolution* or "ACPR") fined the French banks BNP Paribas and Société Générale respectively 10 million euro and 5 million euro for inadequate money-laundering controls.

b. Public record of Ultimate Beneficial Owners (UBO)

Under the law as modified in December 2016, French and foreign companies and corporations were required to identify and register their "ultimate beneficial owner" by August 1, 2017, and must file certain information about those ultimate beneficial owners by April 1, 2018.

An ultimate beneficial owner is broadly defined under French law and can include one or more individuals who ultimately own or control the company or the corporation, or on whose behalf a transaction or an operation is conducted. An individual is considered to own or control the company or corporation if the person holds, directly or indirectly, at least 25% of the share capital or voting rights of the subject company or corporation. An individual or individuals can also be considered an ultimate beneficial owner if he/she/they exercise, by any other means, the authority to control certain functions, including corporate management and governance, control of executive bodies of the company, or hold control over its shareholders' meeting.

The law applies to companies and corporations with a registered office in France, foreign companies with a branch in France, and other legal entities that are required to register in France under legislation or regulations. Companies listed on a regulated market in France or in another EU member state that is a party to the European Economic Area agreement, or in a country imposing similar requirements (such as the United States NYSE) are not subject to this requirement.

Entities subject to the new rules must obtain and keep accurate records of their beneficial owner or owners, must provide this information to the commercial registry upon registration, and then must provide regular updates should the content of the information filed change.

c. Reinforcement of the French Financial Intelligence Unit's prerogatives (TRACFIN)

Created in 1990, TRACFIN (*Traitement du Renseignement et Action contre les Circuits Financiers clandestins,* or Unit for Intelligence Processing and Action against Secret Financial Channels) is a French agency aimed at fighting clandestine financing channels, money laundering, corruption, and terrorism financing. Certain individuals and organizations (such as financial institutions, accounting firms, auditors, insurance companies, and attorneys) are required by law to declare suspicious and potentially corrupt activity, and TRACFIN centralizes and analyzes these declarations. More than half of the investigations into corruption in France are started after the filing of a report of potential misconduct before TRACFIN. If, during the analysis of the information provided, TRACFIN determines that there are indications of corrupt activity, the agency may refer the matter to the prosecutor's office or to special investigation services.

In 2017, 71,070 "pieces of information" were transmitted to TRACFIN, as well as 68,661 reports of suspicious activity, amounting to a 10% increase since 2016, a 57% increase since 2015 and a 160% increase since 2012. TRACFIN conducted investigations or posed further questions on 12,518 of those reports in 2017 (a 8% decrease compared as compared to 2016), and 1,762 investigation requests were sent to foreign investigatory counterparts. TRACFIN sent 2,616 files to French judicial and administrative authorities (a 38% increase since 2016) for further action based on its analysis of reports of suspicious activity.

In December 2016, TRACFIN's powers were expanded, which may explain the improvement of the statistics. For instance, TRACFIN is now vested with the authority to identify any entity subject to its reporting obligations, including any financial operations or persons that may present a high risk of money laundering or financing of terrorism. In addition, TRACFIN's right to postpone the execution of any pending suspicious transactions has been lengthened from five to ten working days. TRACFIN is also now authorized to communicate collected information to several administrative authorities (including customs, tax administration, financial jurisdictions, and the AFA).

3. Increasing the Statute of Limitations for Corruption Offenses

Under French law, criminal offenses fall under three categories depending on their severity: *crimes* (felonies), *délits* (misdemeanors), and *contraventions* (petty offenses). The statute of limitations for felonies and misdemeanors was extended by a new law, passed in February 2017. Following this

reform, the statute of limitations for misdemeanors was extended from three to six years from the day on which the offense was committed.

As an exception, however, the law provides that the statute of limitations for the prosecution of *hidden or concealed* offenses begins to run from the date on which the offense was *discovered* rather than when it occurred. Nevertheless, as a limitation, the prosecution must begin within 12 years (for misdemeanors) and 30 years (for felonies) from the date on which the offense was committed.

IV. Norway

In the past few years, Norway has seen an increase in anti-corruption enforcement efforts and focus on compliance. Norwegian authorities have been proactive in investigating and prosecuting foreign bribery cases, and stakeholder enforcement actions, led by the Council on Ethics for the Government Pension Fund Global ("GPFG" or the "Fund"), have continued to gain momentum. The GPFG has dedicated significant resources to investigating companies that may be involved in gross corruption to determine whether they should be either placed under observation or excluded from the Fund's portfolio. The GPFG has also set the tone for other important stakeholders. For example, Kommunal Landspensjonskasse ("KLP"), Norway's largest insurance company, has adopted Guidelines for Responsible Investment, and has excluded several companies from its portfolio on the basis of the recommendations for exclusion prepared by the Council on Ethics. Such stakeholder enforcement is contributing to the shaping (and elevating) of Norway's position in the international anti-corruption landscape, and is likely to continue to serve as an inspiration for other investment institutions at home and overseas.

A. Investigations and Actions of Note

1. Yara International

a. Background

In January 2014, Yara International ASA ("Yara") agreed to pay NOK 295 million (approximately $48.5 million at the time)—the largest corporate penalty ever imposed on a corporation in Norway—in connection with corrupt payments to government officials in Libya, India, and Russia. Yara is listed on the Oslo Stock Exchange, and is partially owned by the Norwegian government (which holds 36.2% of its shares).

In 2007, Yara's Legal Director Kendrick Wallace orally agreed to pay $4.5 million in bribes to Mohamed Ghanem (the son of the former Libyan Oil Minister) and Dr. Shukri Ghanem (then-Chairman of Libya's National Oil Corporation and *de facto* Oil Minister) in connection with negotiations for a joint venture between Yara and the Libyan National Oil Corporation ("NOC") regarding a joint venture for the production of fertilizers in Libya. At least $1.5 million was paid to a Swiss account held by Mohamed Ghanem.

Yara asked the Swiss company Nitrochem Distribution AG ("Nitrochem") to advance the payment, and refunded Nitrochem through Yara's partially owned Swiss entity, Balderton Fertilizer SA ("Balderton"). The refund was concealed through inflated invoices for several ammonium deliveries from Nitrochem to Balderton between October 2007 and May 2008. The ammonium deliveries were then sold from

Balderton to Yara Switzerland SA for a price, which also included the inflated price Balderton had paid for the raw materials.

In India, in April 2007, Wallace and Yara's Head of Operations, Daniel Clauw, offered to pay an initial bribe of $250,000—which later increased to $3 million—to Gupreetesh Singh Maini. Gupreetesh Singh Maini is the son of Dr. Jivtesh Singh Maini, who at the time served as the Additional Secretary and Financial Adviser in the Ministry of Chemicals and Fertilizers and as a member of the Board of Kribhco. The bribes were offered in connection with the negotiations of a joint venture between Yara and Kribhco.

In both cases, the consultancy agreements entered with the sons of the public officials were fictitious, as these individuals did not have the skills, experience, or independence required to assist Yara. In reality, the role of these individuals was to obtain information and exercise influence on behalf of Yara in the ongoing JV negotiations.

On July 7, 2015, the Oslo District Court rendered a unanimous verdict convicting four former senior executives of Yara: Wallace, Clauw, former CEO Thorleif Enger, and former Head of Upstream, Tor Holba, for paying, aiding, and abetting payments of over $8 million in bribes to family members of public officials in Libya and India in connection with the above conduct. The Court found that the payments constituted an improper advantage provided to senior government officials in connection with a position, office or assignment within the meaning of §§ 276(a) and (b) of the former Norwegian Criminal Code (§§ 387 and 388 of the new Norwegian Criminal Code, which entered into force on October 1, 2015), and found all defendants guilty of gross corruption.

b. Borgarting Court of Appeals

On January 17, 2017, the Borgarting Court of Appeals ("Court of Appeals") jury disagreed with the findings of the Oslo District Court and quashed the convictions of Enger, Holba, and Clauw. Consistent with Norwegian jury trial standards, the Court of Appeals judgment does not include any discussion of the factual and legal basis for the acquittals. Only the grounds for convicting Wallace were discussed as part of the Court's sentencing discussion.

Having agreed with the District Court regarding Wallace, the Court of Appeals proceeded to discuss the appropriate sentencing level. The Court of Appeals observed that Norway's 2003 adoption of new anti-corruption legislation, following its ratifications, *inter alia*, of the Council of Europe Criminal Law Convention on Corruption and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, had generally raised the sentencing level for corruption offenses. In increasing the prison term from two and a half to seven years, the Court of Appeals pointed to several aggravating factors, including (i) the high amount of the payments offered; (ii) the fact that the payments were made to obtain goodwill from public officials that could influence the company's negotiating position with respect to the ventures; (iii) the central role played by Wallace in the corrupt acts, including negotiating and preparing the agency contract in Libya, and organizing the payment through a Swiss company to conceal the relationship with government officials; (iv) the careful planning of the acts of corruption; and (v) the fact that Wallace was the Legal Director, a member of Yara's senior management, and responsible for overseeing Yara's ethical rules and guidelines for business integrity.

With respect to the last point, the Court of Appeals observed that "[a]s the leader of Yara's anti-corruption work, it was [Wallace's] responsibility to ensure that the rules were respected within Yara's organization, and both his skills and role put him in a particularly good place to prevent breaches of anti-corruption laws." The Court of Appeals qualified the fact that Wallace was personally involved in serious acts of corruption as "a significant breach of trust towards the company and its owners," which also led to "reputational damage for the company, and raises questions about the value of Yara's anti-corruption work." While the Court observed that it was clear that Wallace was not at the origin of the scheme, the evidence had not established with certainty who within the organization had ordered the payments. However, the Court found that this should not be given any significant weight, because regardless of who initiated the scheme, Wallace, by virtue of his professional skills and rank within the organization, could have refused to aid and abet the criminal acts without any risk of negative consequences for his position. It was further deemed irrelevant for sentencing purposes whether the acts of corruption were made in a country with a high risk of corruption.

c. Supreme Court Judgment on Sentencing

Wallace sought leave to appeal to Høyesterett, the Norwegian Supreme Court, on the basis of violations of process, incorrect application of the law and the sentence, but was only granted leave to appeal with respect to the latter. On September 15, 2017, the Norwegian Supreme Court upheld the sentence issued by the Court of Appeals.

A central issue before the Supreme Court was whether bribe payments should be viewed with more leniency if made to public officials in countries with high corruption risk. The Court noted that the changes to Norwegian corruption law (including increasing maximum penalties from six to ten years imprisonment), following Norway's implementation of several international anti-corruption instruments, were designed to combat transnational corruption, and that there was no legal basis for differentiating sentences according to the country involved in the corrupt activity. On the other hand, sentences should be assessed in light of the stricter sentencing level adopted by the 2003 law.

The Supreme Court confirmed the Court of Appeals' view that the general increase in sentences for corruption, as well as the presence of numerous aggravating factors, justified the increase in Wallace's sentence. With respect to the Libya affair, the Court noted that the corruption was made with respect to a high-ranking public official (de facto minister), and that Wallace could have refused to aid and abet the acts without any risk to his own position due to the prominence of his position as the Legal Director. The Court also pointed to Wallace's central role in the planning and executing of the corrupt scheme. Wallace decided that the agreement should be oral and took the initiative to make the first illicit payment through a foreign entity to conceal the relationship with the public official and his son. The Supreme Court noted that this confirmed that the corrupt act was carefully planned and intentional. It was also viewed as highly relevant that the amount of bribes promised was very high. The Supreme Court noted that to the extent that an act of corruption is complete from the moment a promise or offer of an improper advantage has been made, no particular weight should be granted to the fact that the full amount never was paid. In the Supreme Court's view, this act qualified for a six-year prison term. With respect to the India-related charge, the corrupt act was also committed in connection with a key public official. Again, Wallace was central in the corruption scheme, as he planned and negotiated the terms of the assignment with the son of the public official. The Supreme Court found that this act alone qualified for a five-year prison term.

For Norway's National Authority for Investigation and Prosecution of Economic and Environmental Crime ("ØKOKRIM"), the acquittal of three of the defendants in its most significant foreign bribery case has been described as a significant step back, after a five-year complex investigation. Following his acquittal, Holba, who had blown the whistle to ØKOKRIM, also criticized ØKOKRIM's decision to prosecute him, stating that the case illustrates the low level of protection of whistleblowers in Norway, and the risk of whistleblowers being prosecuted.

2. Statkraft

In March 2017, Statkraft AS, a fully state-owned Norwegian hydropower company, disclosed that it had informed Norwegian and Brazilian authorities that corrupt acts may have occurred in connection with the activities of its Brazilian subsidiary, the renewable energy company Desenvix Energias Renováveis S.A ("Desenvix" now "SKER"). Statkraft acquired a controlling interest (81%) in Desenvix in 2015. In its 2016 annual report, the company noted that it had initiated an internal investigation related to Desenvix due to Brazil having experienced several corruption cases over the past year. Statkraft indicated that the internal review had found no clear evidence of corruption, but Statkraft had determined to report the case to Brazilian authorities. In addition, Statkraft announced that it had informed ØKOKRIM.

3. Kongsberg Gruppen ASA

In October 2017, the District Court convicted Dag Tore Sekkelsten, the former Head of Sales for Eastern Europe of Kongsberg Defence & Aerospace AS ("Kongsberg Defence"), of gross corruption related to deliveries of communication equipment to Romania between 1999 and 2008. Kongsberg Defense is a subsidiary of Norwegian company Kongsberg Gruppen ASA ("Kongsberg"), which was 50% state-owned at the time of the relevant conduct.

In February 2014, ØKOKRIM charged Kongsberg Gruppen ASA ("Kongsberg"), its subsidiary Kongsberg Defence & Aerospace AS ("Kongsberg Defence"), as well as Mr. Sekkelsten with gross corruption and bribery related to a serious breach of trust, money laundering and gross tax evasion in connection with payments of approximately NOK 180 million (approximately $21 million) through local agents to a General in the Romanian Intelligence Services, a former Deputy Director for Telecommunications of the Romanian Ministry of Interior, and to Mr. Sekkelsten. According to ØKOKRIM, the illegal transfers were made between 2000 and 2006 through a sophisticated network of companies, including companies registered in the Isle of Man, Switzerland, and Saint Vincent and the Grenadines. In 2016, ØKOKRIM dropped the charges against the company due to lack of evidence that the company had been involved in Mr. Sekkelsten's activities, but indicted Mr. Sekkelsten. Separately, two external audit firms hired by Kongsberg each concluded that Kongsberg and Kongsberg Defence had maintained robust compliance programs and had not been involved in Mr. Sekkelsten's misconduct. In October 2017, the District Court convicted and sentenced Mr. Sekkelsten to 4.5 years of imprisonment and confiscation of NOK 14.7 million (approximately EUR 1.5 million). Both Mr. Sekkelsten and ØKOKRIM have appealed the decision, and an appellate hearing has been scheduled for November 2018.

B. Council on Ethics for the Government Pension Fund Global

An increasingly important actor in the Norwegian anti-corruption landscape is the Council on Ethics ("Council") for the GPFG, which recommends whether the Fund should exclude or put companies on observation if there is an unacceptable future risk that the company may contribute to gross corruption. Since 2013, the Council has stated that investigations relating to allegations of gross corruption have become one of its priorities. The recent increase in the number of such corruption cases may have also been driven by the transfer of the final decision-making power from the Ministry of Finance to the Norwegian Central Bank's ("Norges Bank") investment branch, Norges Bank Investment Management ("NBIM" or the "Bank").

1. The Fund and the Ethical Guidelines

The Norwegian GPFG was created in 1990 as a long-term tool for investing current petroleum revenue in order to meet the combined challenge posed by the expected drop of future revenues together with the expected increase in public pension expenditures. The Ministry of Finance owns the Fund on behalf of the Norwegian people. The Ministry of Finance is responsible for the overall management of the Fund and has issued guidelines for its management. The Fund is managed by the Norwegian Central Bank, whose Executive Board has delegated the operational management NBIM.

In September 2018, the GPFG was the world's largest sovereign wealth fund, managing assets of more than $1 trillion, with investments in just over 9,000 companies in 72 countries. It owns approximately 1.4% of the equity of listed companies on a worldwide basis, and 2.4% of the equity of listed European companies.

The Fund invests in equities, bonds and real estate globally. As of June 2018, the fund's asset allocation consisted of 66.8% equities, 30.6% fixed-income securities and up to 2.6% real estate. All companies in the Fund are listed on overseas stock exchanges. The formal framework for the Fund was established by the Norwegian Parliament ("Storting") in the Government Pension Fund Act. The composition of the portfolio is kept secret, but holdings of the Fund, as of December 31, are published in the Annual Report in March of the following year.

2. The Guidelines for Observation and Exclusion from the Government Pension Fund Global

The framework for the management of the GPFG include Ethical Guidelines, which are designed to "remove ethical risk from the [F]und," based on (i) whether the companies (or companies they control) produce or sell certain specified products ("product-based exclusion"), or (ii) whether there is an unacceptable risk that the companies contribute to or are responsible for certain types of conduct that meet certain criteria ("conduct-based exclusion").

With respect to product-based criteria, the Ethical Guidelines provide that the Fund shall not invest in companies that directly or indirectly: (i) produce weapons that violate fundamental humanitarian principles through their normal use; (ii) produce tobacco; (iii) sell weapons or military material to states that are affected by investment restrictions on government bonds; or (iv) mine or produce power and—through themselves or entities they control—derive 30% or more of their income from thermal coal or base 30% or more of their operations on thermal coal.

Under the conduct-based criteria, companies may be put under observation or be excluded if there is an unacceptable risk that it contributes to, or is responsible for: (i) serious or systematic human rights violations such as murder, torture, deprivation of liberty, forced labor and the worst forms of child labor; (ii) serious violations of the rights of individuals in situations of war or conflict; (iii) severe environmental damage; (iv) acts or omissions that, on an aggregate company level, lead to unacceptable greenhouse gas emissions; (v) gross corruption; or (vi) other particularly serious violations of fundamental ethical norms. To enforce these criteria, the Ethical Guidelines provide that the Bank may, at the recommendation of the Council of Ethics, exclude companies from the Fund or place them on observation.

While the Council continuously monitors compliance with all criteria contained in the Guidelines, the Council's practice demonstrates that it generally identifies select annual focus areas to which it devotes significant resources. In 2016, the Council devoted particular attention to the corruption-related criteria, while in 2017, increased attention was dedicated to examining potential violations of human rights, including the use of child labor and working conditions in select industries in South-East Asia as well as the situation for migrant workers in the Gulf States. The Council also assessed companies involved in activities known as shipbreaking or "beaching," which involves the disposition of vessels to be broken up for scrap on the beaches of Bangladesh and Pakistan, with negative human rights and environmental impacts. In 2017, 69 companies were assessed in connection with these two human rights-related criteria, three of which were recommended for exclusion and one for observation. In 2017, nine companies were evaluated based on the corruption criterion. By March 1, 2018, the Fund had excluded one company for corruption, and the three others were placed on observation.

3. Investigations by the Council of Ethics

The Council, which investigates potential violations and provides recommendations to Norges Bank regarding exclusion and observation, is an independent advisory council that was established by Royal Decree in 2004. It is composed of five members, including a Chair and Vice Chair, appointed by the Ministry of Finance upon recommendation by the Bank for a period of four years. Five new Council members were appointed in December 2014 for a term of four years, and the Council is presently led by Johan H. Andresen, a Norwegian industrialist and philanthropist. The Council's members notably include the current Secretary General of Transparency International Norway. The Council is assisted by a secretariat, which administratively is located within the Ministry of Finance.

The Council is vested with the responsibility to monitor continuously the Fund's portfolio to identify companies that contribute to or are responsible for conduct that may justify observation or exclusion (described below). The Council encourages individuals and organizations to provide information about cases that may be of relevance to its work, but as an advisory body, it is not bound to investigate these. The Council either investigates matters on its own initiative or at the request of the Bank. To date, the identification of companies to investigate has been through systematic reviews of problem areas and sector studies, reports received from special interest groups, news monitoring, and employing an external firm of consultants that carries out daily online searches in several languages to find news items about companies in the portfolio. The Council is working to develop a methodology for the monitoring of the new conduct-based criterion relating to companies involved in greenhouse gas emissions, and the Council uses external consultants to monitor companies whose activities may contravene the weapons and tobacco criteria. In an effort to establish a more transparent and coherent

process for initiating investigations, the revised Ethical Guidelines require that the Council develop and publish principles for the selection of companies subject to "closer investigation," and the Bank may adopt "more detailed expectations relating to these principles."

After identifying a company for investigation, the Council obtains information from research institutions as well as national, regional, and international organizations, and then assesses the specific allegations in light of the requirements of the Ethical Guidelines. The Council typically engages in a dialogue with companies under investigation and grants them an opportunity to present information and viewpoints to the Council at an early stage of the process. Where the Council decides to recommend an observation or exclusion, the company will be permitted to provide their views on draft recommendations prior to their submission to the Bank.

The Council has adopted a regional and sectorial risk-based approach to investigating corruption cases, focusing on companies that work in sectors that are perceived to be particularly corruption-prone according to international rankings, such as the construction, oil and gas, defense and telecommunication industries within countries perceived to have high corruption risks. The Council prepares a publicly available annual work plan defining priorities for its work, as well as an annual report on its activities, both of which must be submitted to the Ministry of Finance. In its 2016 report, the Council stated that in 2016, it had prioritized corruption-related cases, with several sectoral studies having been completed. It further announced that it was in the process of opening a new sectoral study of the pharmaceuticals sector.

Importantly, the Ethical Guidelines, as revised in 2014, provide for enhanced coordination and exchange of information between the Bank and the Council. The changes appear designed to address previous criticisms of inefficiency and delays in the Council's investigative process and to prevent the Bank and Council from adopting what has been perceived, in the past, as inconsistent and conflicting approaches to the implementation of the Fund's responsible management policy. In addition to conducting regular meetings to coordinate their work and exchange information, the Bank and the Council are now required to coordinate their communications with companies to ensure that these are perceived as consistent. To this end, the Bank may access the Council's communications and meetings with companies, and it may integrate such communications into its general follow-up of the companies in its portfolio. The Guidelines require that the Bank and the Council formalize the process through the adoption of detailed procedures for the exchange of information and coordination to clarify their respective roles and responsibilities.

In an effort to promote transparency and responsible investment, the Bank publishes all decisions under the Ethical Guidelines with corresponding Council recommendations. The Bank is also required to maintain a public list of companies excluded from the Fund or placed under observation (described below).

4. Potential Actions from Investigations

a. Exclusion

In the most extreme cases, the Bank can determine to exclude a company from its portfolio if the investigation reveals significant violations. Companies are not excluded for a defined period of time and may be readmitted into the portfolio as soon as the grounds for exclusion no longer exist. Every year, the

Council makes a cursory assessment of excluded companies to determine whether circumstances have materially changed.

The Ethical Guidelines provide a list of general factors the Bank must assess in determining whether to exclude a company. These include: (i) "the probability of future norm violations; (ii) the severity and extent of the violations; (iii) the connection between the norm violation and the company in which the Fund is invested; (iv) the breadth of the company's operations and governance, including whether the company is doing what can reasonably be expected to reduce the risk of future norm violations within a reasonable time frame; (v) the company's guidelines for, and work on, safeguarding good corporate governance, the environment and social conditions; and (vi) whether the company is making a positive contribution to those affected, currently or in the past, by the company's conduct." The threshold for exclusion has been described by the Council as "intentionally high," and it should be limited to those situations where companies "represent an unacceptable future risk to the fund's ethical standards."

With respect to gross corruption, the Council also considers whether (i) the amount, the frequency, and systematic nature of the allegations constitute gross corruption, and (ii) there is an unacceptable risk that gross corruption will continue in the future. The Council will recommend exclusion when both of these criteria are met. While not formally binding upon the Council, gross corruption is broadly defined to cover aggravated corruption within the meaning of §§ 387 and 388 of the Norwegian Criminal Code, and it encompasses both active and passive corruption. Initially, the Council performs a thorough assessment of the corruption allegations that have been made against a company. The Council then proceeds to the assessment of whether there is a risk that the company will continue such practices in the future. This assessment is deemed critical for purposes of exclusion.

The key to the second part of the test for exclusion due to gross corruption is whether the company has implemented an effective anti-corruption compliance program. On this point, the Council bases its assessment on established international norms and best practices. The Council considers these to include existing FCPA and UK Bribery Act guidance and practice, the UN's anti-corruption portal TRACK, the UN Global Compact, the OECD's Good Practice Guidance on Internal Controls, Ethics and Compliance, and Transparency International's Business Principles for Countering Bribery. The Council places particular importance on the way in which the company responds to allegations of misconduct and whether individuals who knew or should have known about misconduct have been removed from their positions. In addition, the Company gives significant weight to the implementation of an effective compliance program, how these are managed internally and communicated externally, the degree to which they are effectively implemented, and the ways in which the company has organized and staffed its anti-corruption work.

In practice, companies involved in corrupt activities must demonstrate that they have developed an effective compliance program and devoted appropriate resources to this work such that the Council is satisfied that the risk of future corruption has been sufficiently reduced so that the company need not be excluded from the Fund. Among other things, the Council views the performance of systematic risk mapping and assessment of risk as a prerequisite and the foundation of an anti-corruption program. In its experience, companies that have been able to assess risk effectively have conducted extensive internal reviews of corruption allegations with the assistance of external parties that are given sufficient resources and autonomy to shed light on the misconduct. The Council also places considerable importance on

adopting an appropriate tone at the top. For the tone to be credible, management must not only take every opportunity to communicate their attitude towards corruption both internally and externally, but it must also point to specific examples of former employees irrespective of position or role, being subject to sanctions, to reinforce the message that the rules apply to employees at all levels.

b. Formal Observation

The Council has the authority to put companies under formal observation if, for instance, there are doubts as to whether the conditions for exclusion (discussed above) have been fulfilled or there is any other uncertainty about the situation. The Council has stated that placing a company under observation "signals that a company has come very close to exclusion," and that the Council will continue to monitor the company's activities. The observation mechanism allows for a more dynamic approach, in which the Council may positively influence a Company's conduct. During an observation period in connection with allegations of gross corruption, the Ethics Council monitors (i) the development of the company's compliance programs, (ii) its implementation of remedial measures to address past misconduct, and (iii) any new allegations of corruption. Where new violations are identified, or where the company fails to implement effective measures to reduce the future risk of non-compliance, the conditions for exclusion (discussed more fully below) may be met.

c. Active Ownership

An important feature of the Ethical Guidelines is that they require the Bank to consider whether other measures, including the active exercise of ownership rights, may be better suited to reduce the risk of future violations prior to making a determination of whether to observe or exclude a company. The Bank is required to consider all alternative measures at its disposal and shall apply these in a coherent manner. This requirement is reflective of the Council's practice to date, pursuant to which the Council has viewed exclusion and observation as a last resort, preferring instead to mitigate risks when possible by encouraging companies to implement sufficient remedial measures. At the same time, the Council has viewed the criteria for exclusion as a significantly "high threshold" that would only apply to a few companies. In his introduction to the 2016 Annual Report, the Chairman of the Council noted that while the "Council on Ethics has been busier than ever in 2016, […], I am pleased to note that this has not resulted in a record number of exclusions. For we have seen that companies are increasingly keen to avoid being excluded. During the course of their dialogue with us, several of them have altered their management systems and business practices, or have improved their level of compliance with their own guidelines. This has made us more confident that the risk of future ethical non-compliance, which is what we have been tasked with assessing, has been reduced." Indeed, the Council does not seek to become a new enforcement agency, but rather seeks a softer and result-oriented approach based on cooperation and dialogue to encourage companies to refrain from corrupt activity. On this point, the Chairman noted that the Council would be "just as happy when companies that are in a dialogue with the Council or Norges Bank alter their conduct and thus themselves reduce the risk of a future violation of the criteria."

5. Specific Corruption Cases 2016 – 2018

From 2016 to 2018, the Council on Ethics has issued recommendations with respect to the observation or exclusion of six companies. As described below, two companies were placed under observation (PetroChina and Leonardo SpA), and two were recommended for exclusion (ZTE Corporation and JBS SA), while for two others Norges Bank announced its decisions to ask NBIM to

follow up on the risk of corruption in its ownership dialogue with the companies (Eni SpA and Saipem SpA).

- *Observation of PetroChina (May 5, 2017):* On December 8, 2016, the Council on Ethics recommended the exclusion of PetroChina, a Chinese oil production and distribution company, from the GPFG due to the risk of gross corruption. The Council's review found that more than 65 senior executives and middle managers formerly employed by PetroChina and its subsidiaries were under investigation for allegedly receiving bribes in China, Canada and Indonesia during the period of 1980 to 2014, with 18 of these individuals believed to have been formally sanctioned and/or convicted of corruption by Chinese authorities. Between 2015 and 2016, the Council engaged in a dialogue with PetroChina to better understand the circumstances of these allegations. However, PetroChina did not provide sufficient information nor did it provide any comments to the draft recommendation. The Council noted that PetroChina had improved its anti-corruption compliance systems since 2014, but that it had failed to provide sufficient information about how the program would be implemented or substantiate how these would function effectively throughout the organization. Viewed in conjunction with the fact that PetroChina's current management is largely the same as when the corrupt practices were alleged to have taken place, and that the size of the bribe payments received was so high that the management knew or should have known, the Council found that there was a high future risk of future misconduct. The Council cited to Report No. 20 (2008 – 2009) to the Norwegian Storting, which states that a company's lack of willingness to provide relevant information, in and of itself, contributes to the risk of being complicit in unethical behavior being deemed unacceptably high, and recommended that PetroChina be excluded from the Fund's portfolio. However, in its decision on May 5, 2017, Norges Bank found that the fact that the Council highlighted that PetroChina had taken measures against corruption provided sufficient grounds to continue to observe future developments, and placed PetroChina under observation. The Council of Ethics will follow up on the risk of corruption with PetroChina while it is under observation.

- *Observation of Leonardo SpA (May 5, 2017):* On December 8, 2016, the Council on Ethics recommended the exclusion of Leonardo SpA ("Leonardo"), an Italian industrial group active in the sale of aircraft, defense and security equipment, from the GPFG due to the risk of gross future corruption. The Council observed that Leonardo had been involved in serious cases of corruption, alleged to have been taken place in India, South Korea, Panama and Algeria during the period from 2009 and 2014. The Council noted, *inter alia*, that former Chair of Leonardo's Board of Directors and its former CEO were sentenced to prison for gross corruption in connection with a contract in India. From 2014 to 2016, the Council engaged in active dialogue with Leonardo, which provided information on the matter and submitted comments to the draft recommendation. At the outset, the Council noted that despite Leonardo having changed its management team, the Council presumed that "in a company where senior management is involved in the circumvention of its own routines, there is reason to believe that the risk of non-compliance is substantial, and that more is required to alter the prevailing corporate culture than in companies where corruption occurs further down in the organization and is more sporadic," and that "[t]he company's attitude towards the allegations gives the impression of an attempt to sidestep its corporate responsibilities." The Council noted that following widespread allegations of corruption, in

2013 Leonardo initiated significant changes to its management and established a committee of experts to offer advice on how to improve its anti-corruption compliance program. However, the Council was not satisfied that the program was working effectively to prevent future violations. In particular, the Council found that at the same time that Leonardo established the expert committee, it continued to enter into agreements in violation of internal guidelines, including by not performing appropriate third-party due diligence. With respect to risk assessments, the Council stated that performing a one-off risk assessment in 2015 was not sufficient to substantiate that the Company evaluates and mitigates corruption risk on a regular basis. The Council also criticized the failure to provide a detailed plan for how the company intended to scale back the use of agents and the failure to provide appropriate anti-corruption training to such agents. Finally, while Leonardo established a new whistleblower line in 2015, the fact that the company explained that it had never received a single report could, in the Council's view, be a sign that the anti-corruption efforts were not appropriately communicated throughout the organization, that employees were not encouraged to report their concern or that the line did not function properly. The Council therefore recommended that Leonardo be excluded from the portfolio of the Fund. On May 5, 2017, however, Norges Bank announced that it had determined to followup on these issues through active ownership dialogue with Leonardo.

- *Recommendation for exclusion for ZTE Corporation (January 7, 2016)*: On June 24, 2015, the Council on Ethics recommended the exclusion of ZTE Corporation ("ZTE"), a Chinese telecommunications equipment company, from the GPFG due to an unacceptable risk of gross corruption. The Council observed that ZTE was under formal investigation for corruption in 10 different countries, including Algeria, Kenya, Papua New Guinea, Zambia, the Philippines, Malaysia, Myanmar, Nigeria, and Liberia. The Council noted that all of the corruption allegations against ZTE involved the bribing of public officials, often to obtain contracts. ZTE had also been involved in allegations of corruption in nine other countries, including Ethiopia, the Democratic Republic of Congo, Tajikistan, Kazakhstan, Kirgizstan, Mongolia, Thailand, Pakistan and India. The corruption allegations existed over an extended period of time, dating from 1998 to present day. With the exception of the cases in Papua New Guinea, the Philippines, Kenya and Liberia, the Council noted that the allegations were impossible to confirm through official court documents or investigation documents because they took place in countries where such information is usually not made public. Among the above-mentioned investigations, the Council found that two ZTE executives were convicted of corruption in Algeria in 2012 for bribing public officials in connection with the awarding of contracts in Algeria between 2003 and 2006, and they were sentenced *in absentia* to 10 years of prison and a fine of $65,000. ZTE's subsidiary ZTE Algérie was also fined and banned from participating in public tenders in Algeria for two years. In Zambia, the Zambian Anti-Corruption Commission (ACC) confirmed accusations of corruption by ZTE's representatives in order to obtain a contract without a public tender in 2011. The value of the contract was estimated at $210 million. The Council evaluated ZTE's anti-corruption procedures in light of international standards for corporate anti-corruption systems. Despite finding that ZTE had an internal compliance program, the Council concluded that, given the large number of corruption cases in which ZTE appears to have been involved, ZTE executives "must or should have known about the corrupt practices." The Council also noted

that was unclear what consequences employees would face if they breached either internal guidelines or national laws. In its communication with the Council, ZTE provided limited information on its anti-corruption efforts, and sometimes failed to respond entirely. The Council thus deemed that there existed an unacceptable risk of gross corruption regarding ZTE and recommended that the company be excluded from the portfolio of the fund. Norges Bank decided to follow the Council's recommendation to exclude ZTE on January 7, 2016.

- *Recommendation for exclusion for JBS SA (July 10, 2018):* On March 1, 2018, the Council on Ethics recommended the exclusion of JBS SA ("JBS"), a Brazilian company that is the second largest food company and largest meat producer in the world, from the GPFG due to an unacceptable risk that the company is responsible for gross corruption. Over the last 10-15 years, former members of JBS' management and board of directors admitted to bribing 1,829 politicians from 28 different political parties in Brazil. This was done primarily to obtain public financing, tax breaks or other financial benefits to facilitate the growth of JBS' business. The politicians implicated in receiving the bribes include 167 members of the Brazilian Parliament, 16 District Governors and two previous Brazilian Presidents. The bribes paid amount to approximately NOK 1.5 billion (about $185 million). On May 18, 2017, the Brazilian Supreme Court authorized a plea bargain agreement between the prosecuting authorities and JBS' Board Chair and CEO, as well as five other people associated with JBS or J&F (a family-owned holding company that owns about 42% of shares in JBS). Although the Council acknowledged that Brazil itself has a historical and structural problem with corruption, it noted that anti-corruption legislation was passed in 2013 and anti-corruption measures have been added to the Brazilian Penal code, which address both active and passive corruption. The Council stated that, in light of the corruption allegations against it, JBS should have investigated the allegations either in their early stages or later on. Further, JBS did not make any efforts to prevent new incidents of corruption. JBS also originally denied the allegations that the Board Chair and the CEO had bribed public officials and never suspended them, even when the company came under investigation by the government. The CEO was only removed once he was arrested in September 2017. Furthermore, JBS did not launch internal reviews of the allegations. In its communication with the Council, "JBS made it clear that it cannot guarantee that members of the family, which is its major shareholder, will not continue to hold key positions in company management." Indeed, in 2017, JBS' board yet again appointed a close family member as CEO. The second-largest shareholder of JBS, BNDES "publicly criticized the circumstances surrounding the decision" and stated it considered JBS' corporate governance unsatisfactory. Considering that JBS did not have a far-reaching plan for combatting corruption in place until May 2017, and in light of the scale and seriousness of the corruption scheme to which JBS eventually admitted, the Council concluded that there remained an unacceptable risk of gross corruption associated with JBS and recommended its exclusion. Norges Bank decided to exclude JBS on July 10, 2018.

- *Eni SpA Not Included on the Fund's Observation List (May 5, 2017):* On December 20, 2016, the Council on Ethics recommended that Eni SpA ("Eni"), an Italian multinational integrated oil company, be placed under observation due to future risk of gross corruption. The Council observed that Eni and several of its former senior executives had been or currently were under investigation by American, Italian and Nigerian authorities in connection with corruption allegations in Nigeria and Algeria. The Council engaged in a dialogue with Eni through written communications and meetings from 2015 to 2016, during which Eni represented that it had

significantly enhanced its compliance program and commented upon the draft recommendation. The Council nonetheless reached the conclusion that Eni had not substantiated that its anti-corruption program would be effectively implemented throughout its operations. Eni was criticized for having a questionable tone at the top, referencing the 2014 promotion of a senior executive that had since been indicted for corruption in Algeria by Italian prosecutors, and the investigation for gross corruption of the sitting CEO. Additionally, the Council found that Eni did not have appropriate corruption risk assessment processes, nor did it assess the effectiveness of its training programs. While the Council noted that in principle the conditions for exclusion were met, in light of Eni's recent enhancements to its compliance program, including the creation of a new compliance organization and its reduced shareholding in Saipem (a subsidiary through which the conduct in Algeria is alleged to have taken place), the Council recommended to put Eni under observation. On May 5, 2017, however, Norges Bank announced that it had determined to followup on these issues through active ownership dialogue with Eni.

- *Saipem SpA Not Included on the Fund's Observation List (May 5, 2017):* On December 20, 2016, the Council on Ethics recommended that Saipem SpA ("Saipem"), an Italian multinational oil services company, be placed under observation due to future risk of gross corruption. The Council noted that Saipem was under investigation for corruption in several countries, including Nigeria, Algeria, Brazil and Kuwait. While the Council engaged in active dialogue with Saipem between 2014 and 2016, through both written communications and meetings, and Saipem provided comments to the draft recommendation, the Council still found that Saipem had failed to substantiate that it had an effective compliance program in place. In particular, and despite Saipem having undertaken measures to implement a new compliance program and remove all individuals implicated in the investigations from its management team, the reported allegations and Saipem's risk assessments led the Council to conclude that it was uncertain whether Saipem's current anti-corruption program would effectively prevent corruption in the future. However, the Council recommended that Saipem be placed under observation, given that Saipem had recently made substantial changes to its anti-corruption program and to its management group, and that Saipem was in the process of assessing the status of implementation of the program within several important subsidiaries, with the help of an external consultant. The Council therefore recommended reevaluating the situation in a couple of years. Norges Bank did not follow the Council's recommendation, and instead announced on May 5, 2017 that it had decided to ask NBIM to follow up on the risk of corruption in its active ownership dialogue with the company.

C. Kommunal Landspensjonskasse

Norway's largest insurance company Kommunal Landspensjonskasse ("KLP"), has also adopted Guidelines for Responsible Investment, allowing KLP to use exclusion to eliminate companies that can be linked to gross and/or systematic violations of generally accepted norms for business conduct, including gross corruption, from its investment portfolio. The KLP Guidelines do not include an observation mechanism. As of September 2018, companies excluded on the basis of gross corruption were Centrais Eletricas Brasileiras SA (2016), China Railway Group Ltd (2015), JBS SA (2018), Leonardo SpA (2017), PetroChina (2017), Petrobras (2016), and ZTE Corporation (2016). Several of these were excluded based on the Council's May recommendations to exclude. Interestingly, even though the Fund did not

necessarily end up excluding the companies, these companies were excluded by KLP. In total, KLP has excluded 199 companies for violations of KLP's Guidelines for Responsible Investment.

D. OECD Phase 4 Report

1. Overview

On June 14, 2018, the OECD Working Group on Bribery published its Phase 4 report on Norway's implementation and enforcement of the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and related instruments. The Working Group observed an overall robust legal framework in Norway regarding active anti-bribery enforcement. Nevertheless, since its last Phase 3 evaluation in 2011, the Working Group raised concerns regarding certain aspects of Norwegian law. These primarily relate to (i) amendments to the provisions regarding jurisdiction introduced in the 2005 Penal Code that it fears may weaken enforcement, (ii) uncertainty regarding the scope of corporate liability. Below we describe some of the key takeaways from the Working Group Report.

2. Active Enforcement Efforts and Extensive Cooperation with Foreign Authorities

The OECD Working Group noted positively that Norway has actively enforced its foreign bribery laws. ØKOKRIM investigated ten of the twenty-three allegations of foreign bribery that have arisen since the Anti-Bribery Convention entered into force in 1999, five of which resulted in sanctions against at least one defendant. Two of the investigations remain ongoing, while the other three were discontinued. Norway's extensive use of formal and informal international cooperation mechanisms were also commended by the Working Group.

3. Self-Reporting

The Working Group noted positively that self-reporting by companies has become an important and reliable source of information for Norwegian authorities in detecting potential foreign bribery offenses. The Working Group stated that self-reporting by companies was the source of three of the four cases that resulted in sanctions for legal persons. Although self-reporting is encouraged, the Working Group noted that it is unclear how, and to what extent, such reporting will benefit companies. While Section 78 of the Penal Code allows judges and prosecutors to reduce the sanctions imposed on companies that self-report, it does not protect against other sanctions such as for example debarment from government contracting and exclusions from public advantages. Therefore, companies that depend on public procurement would be more reluctant to self-report. Indeed, companies reported that they were uncertain about the extent to which their sanction would be reduced because of the self-reporting. Therefore, the Working Group recommended that Norwegian authorities clarify the application of outcomes and procedures for self-reporting instances of foreign bribery.

4. Limited Jurisdiction Over Acts of Corruption Committed Overseas

While the previous Phase 3 review had found that Norway enjoyed broad jurisdiction over foreign bribery offenses, the Phase 4 review revealed that the introduction of a "reciprocity condition," which has the effect of limiting Norway's jurisdiction over foreign bribery acts that occur abroad to those acts that are

"also punishable under the law of the country in which they are committed," has restricted the country's jurisdiction over corruption offenses committed abroad. Although Norway maintains territorial jurisdiction over foreign bribery acts that occur in Norway, the changes to the Penal Code have removed its "universal jurisdiction," which allowed Norwegian authorities to exercise jurisdiction over corruption offenses committed by foreigners abroad if the King gave his consent. Under the new Penal Code, Norway can assert nationality jurisdiction over offenses committed abroad by natural and legal persons that have "a sufficient connection" with Norway. This includes individuals who were Norwegian nationals or residents at the time of the offense, as well as those who become a Norwegian national or resident after committing an offense. With respect to legal persons, Norway can exercise jurisdiction over acts committed "on behalf of an enterprise registered in Norway", as well as over acts committed on behalf of a foreign company that later transfers its entire operation to an enterprise registered in Norway.

However, the new Penal Code provides that nationality jurisdiction for corruption offenses may be limited to acts that are "also punishable under the law of the country in which they are committed." This means that the act must not only be unlawful in the place where it was committed, but also that the offender must still be subject to punishment in that jurisdiction. As a result, Norway could be prevented from prosecuting a defendant who could assert a defense that is permitted in the foreign jurisdiction, such as the expiry of the relevant statute of limitations for an offense, even if that defense is not recognized under Norwegian law. The Working Group noted that this condition to asserting nationality jurisdiction could have a negative effect on Norway's prosecution of foreign bribery offenses committed abroad. It therefore recommended that Norway amend the Penal Code to ensure that it can prosecute foreign bribery offenses committed by its nationals abroad without the condition of the act being unlawful or punishable in the jurisdiction where it was committed.

The new Penal Code also affects Norway's ability to impose sanctions on foreign bribery offenses. Under the new Penal Code, any penalty imposed "may not exceed the maximum statutory penalty for a corresponding act in the country in which it has been committed." The Working Group noted that this restriction could potentially limit Norway's ability to impose effective, proportionate and dissuasive sanctions on its own citizens and companies. It was therefore recommended that Norway modify the Penal Code's provisions that limit its sanction power to those that would be available in the jurisdiction where the crime occurred. The Working Group recommended that Norway ensure it can assert nationality jurisdiction over foreign bribery offenses committed abroad and clarify its legal framework for foreign bribery enforcement.

5. Uncertainty Regarding the Scope of Corporate Criminal Liability

The Working Group noted that Norway's current corporate liability framework imposes discretionary liability for companies and could benefit from a more fully defined liability framework, both with respect to the potential liability for acts of subsidiaries, as well as how mitigating actions can limit liability and associated criminal fines.

a. Liability for the Acts of Foreign Subsidiaries and Other Intermediaries

Under Section 27 of the Penal Code, companies can be held liable for a violation committed by any natural person acting on its behalf. However, the Working Group noted that its review revealed uncertainty about the exact scope of corporate liability when corruption is committed by foreign

subsidiaries and other intermediaries due to the lack of definitive jurisprudence to indicate when a person is acting on behalf of a legal person. The legislative history to the new Penal Code indicates that the natural person must have some connection to the parent company. This Working Group observed that that the extent to which companies will be held liable for the acts of intermediaries, which include related entities such as foreign subsidiaries, could be further clarified.

b. Discretionary Use of Corporate Criminal Liability

While criminal liability *may* be imposed on corporations, this is not mandatory, but is left at the discretion of Norwegian prosecutors when the conditions of Section 27 are met. In particular, Prosecutors make an overall assessment of whether the company should be charged and, if so, which sanctions should be imposed, based on an eight-factor list provided in Section 28 of the Penal Code. Among the considerations included in the list are the deterrence and prevention of the offenses, the severity of the offense, whether the offense was committed to promote the interests of the enterprise, and the company's financial capacity. Section 78 of the Penal Code also provides a non-exhaustive list of mitigating circumstances that are relevant to the imposing of sanctions. These include, *inter alia*, whether the offender has made an "unreserved confession" or contributed to solving other offenses. The Working Group noted, however, that the application of these mitigating factors in practice is unclear. It was therefore recommended that the application of mitigating measures be further clarified, as little guidance is available to the business community and public concerning their application. Clarifications by Norwegian authorities on the scope of corporate liability, as well as on the application of sanctions and their possible mitigating factors, will help the business community more fully understand the nature and scope of their legal obligations and encourage their compliance with these obligations. This is also consistent with feedback from Norwegian companies, who have long requested further guidance from enforcement authorities regarding the expectations of enforcement authorities with respect to compliance programs, self-reporting and other remedial measures.

Similarly, the Working Group noted that further guidance is needed regarding the use of penalty notices (*i.e.* corporate criminal fines) in Norway. Penalty notices allow the prosecutor to resolve a case without going to trial under certain circumstances, with the agreement of the accused offender. The Working Group noted that the Phase 3 review had made the use of penalty notices a follow-up issue, but that the Criminal Procedure Act ("CPA") provisions regarding penalty notices remained unchanged since Phase 3. While the Working Group noted that the Director of Public Prosecutions had issued guidance for prosecutors on the use of penalty notices, it noted that further guidance is needed, particularly on penalty notice procedures and the range of possible outcomes. It was recommended that guidance be addressed to business managers and legal practitioners, and that as much information as possible be made public about accepted penalty notices.

CHAPTER 5: MULTILATERAL DEVELOPMENT BANKS

I. Context

Multilateral Development Banks ("MDBs") continue to play an important role in the global fight against corruption and, as in past years, the effort is spearheaded by the World Bank. As of the end of the 2017 fiscal year, the World Bank Group alone sanctioned 60 entities and individuals and honored 84 cross-debarments originating from sanctions imposed by other MDBs.

The World Bank first expanded its anti-corruption capabilities following the seminal "cancer of corruption" speech by the Bank's then-President James D. Wolfensohn in October 1996. Almost 20 years later, in December 2013, the World Bank's current president Mr. Jim Yong Kim reaffirmed the Bank's commitment to fighting corruption by boldly declaring corruption to be "public enemy number one." Among other things, President Kim has led a major restructuring effort of the Bank, which included creating a "Governance Global Practice" intended to act as "a single pool of technical experts in rule of law, public sector, financial and state management, and public procurement." Supporting anti-corruption and transparency initiatives in over 100 countries, and counting over 750 staff members, the Governance Global Practice is now one of the largest of the World Bank's global practices.

The focus of the World Bank's anti-corruption efforts is the Bank's sanctions regime, encapsulated in the "Sanctions Procedures." The sanctions regime was created shortly after President Wolfensohn's cancer of corruption speech and has undergone (and continues to undergo) a series of revisions and improvements.

The sanctions regime gives the World Bank the ability to investigate and sanction firms and individuals for "sanctionable practices" (*i.e.*, fraud, corruption, collusion, obstruction, and coercion) committed during the procurement or implementation of World Bank-financed projects. Depending on the gravity of the misconduct, a range of sanctions may be imposed, including letters of reprimand (generally reserved for minor misconduct), debarment with conditional release (the baseline sanction, recommended in most cases) and indefinite debarment from participating in any future World Bank-financed projects (reserved for the most severe misconduct). The World Bank's jurisdiction is contract-based. The Sanctions Procedures apply whenever a contract between a borrower and the World Bank is governed by the Bank's Anti-Corruption, Procurement or Consultant Guidelines. The World Bank's sanctions regime mainly focuses on contractors, subcontractors, and consultants and does not cover public officials of governments. The sanctions regime also does not cover World Bank staff members who have engaged in misconduct. World Bank staff members are subject to separate administrative proceedings.

The World Bank regime is the most mature of—and serves as the de facto model to—the sanctions regimes of other MDBs. In fact, over the course of the past decade, there have been a number of initiatives to harmonize various MDB sanction regimes and increase cooperation between MDBs. For instance, on September 17, 2006, the World Bank, the African Development Bank ("AfDB"), the Asian Development Bank ("ADB"), the European Bank for Reconstruction and Development ("EBRD"), and the Inter-American Development Bank ("IADB") entered into a landmark agreement that, among other things, harmonized their definitions of fraudulent and corrupt practices and their investigative processes. The resulting cooperation was further enhanced by the April 2010 Agreement for Mutual Enforcement of Debarment Decisions—commonly referred to as "Cross-Debarment Agreement"—between the AfDB,

ADB, EBRD, the IADB, and the World Bank, pursuant to which debarments greater than one year in length issued by one participating MDB trigger cross-debarments by the other participating MDBs. In March 2017, the Asian Infrastructure Investment Bank ("AIIB")—the newest of the MDBs, which was declared open for business on January 16, 2016—demonstrated its commitment to developing an effective sanctions regime by announcing that it had voluntarily adopted the list of sanctioned firms and individuals maintained under the Cross-Debarment Agreement and is seeking to become a party to the Agreement along with the five other MDBs.

II. Why the MDB Sanction Process Matters From a Business Perspective

Far from being only a theoretical Damocles' Sword, sanctions regimes have started to be actively implemented by most MDBs. Indeed, according to official fiscal year 2017 statistics published by the World Bank's investigatory body, the World Bank reviewed 166 contracts and 68 projects, worth $818 million, pursuant to allegations of sanctionable practices. According to other official statistics, the World Bank sanctioned a total of 489 individuals and firms through its Sanctions Procedures between fiscal years 2008 and 2017 (excluding cross-debarments from other MDBs and affiliates of sanctioned firms).

The continued importance of sanctioning activity, the potential disruptions caused by the sanctions procedures, as well as the severity of sanctions, underscores the need for companies operating in the development sector to familiarize themselves with the respective sanctions regimes of the MDBs.

III. Overview of MDB Sanctions Regimes

A. World Bank Sanctions Regime

The World Bank's current sanctions regime is set out in full in the "Bank Procedure: Sanctions Proceedings and Settlements in Bank Financed Projects," issued on June 28, 2016, with an effective date of January 7, 2016 ("Sanctions Procedures"). As per explanatory notes found in the Sanctions Procedures themselves, as well as recently issued World Bank Sanctions Board decisions, the new Sanctions Procedures are a "re-adopted" and "retrofitted" version of the previous April 15, 2012 procedures. The World Bank did not widely publicize the issuance of the new Sanctions Procedures, as the modifications largely consisted of changing the structure and numbering of the paragraphs, as well as updating the terminology used (for example, switching the outdated term of "Evaluation Officer" to "Suspension and Debarment Officer" or "SDO"). While no significant substantive changes were undertaken, the World Bank did take the opportunity to clarify certain points, notably by introducing a new section on the "Rules on delivery and submission of notices and other materials in World Bank Sanctions Proceedings," mentioned further below.

1. Investigation and Adjudication: Main Actors and Process

The core of the World Bank's sanctions regime is built around three main actors and their respective responsibilities: the Integrity Vice Presidency, the Office of Suspension & Debarment and the Sanctions Board, which respectively represent the Bank's investigatory branch and two adjudicatory bodies.

Integrity Vice Presidency (INT): INT is a World Bank internal body, whose main responsibility is investigating allegations of sanctionable practices on Bank-funded projects. Such allegations are mostly

reported to INT by government officials of the borrowing country (*e.g.*, members of the implementation agency or the bid evaluation committee), World Bank staff participating in the project, or other types of whistleblowers (*e.g.*, competitors). Typically, once INT has concluded its investigation and finds that there is sufficient evidence supporting the allegations of sanctionable practices, INT summarizes its findings in a "Statement of Accusations and Evidence" and refers the case to the Office of Suspension & Debarment for first-level adjudication.

Office of Suspension & Debarment (OSD): The OSD, headed by the Suspension and Debarment Officer (or SDO), acts as the initial (and, often final) adjudicator of cases brought to it by INT. The OSD determines if the evidence supports a finding of a sanctionable practice under the applicable World Bank Procurement, Consultant or Anti-Corruption Guidelines and, if so, may recommend the imposition of sanctions by issuing a "Notice of Sanctions Proceedings" to the respondent. If the respondent does not contest the OSD's recommended sanctions, the sanctions are imposed as recommended and the OSD's decision is published on the OSD's website. If the respondent wishes to contest the recommended sanctions, the respondent can do so through two non-exclusive options. The respondent may, within 30 days of receipt of the Notice, submit a written "Explanation" to the OSD, who, upon review of the Explanation, can either (i) maintain the initial recommendation, (ii) revise the recommended sanctions or (iii) withdraw the Notice. The OSD's decision may then, in turn, be appealed before the Sanctions Board. The respondent can also chose to bypass the OSD and file a written "Response" directly with the Sanctions Board, within 90 days of the receipt of the Notice. At the end of fiscal year 2017, two-thirds of all cases (66%) were resolved at the level of the OSD and only one-third (34%) proceeded to the Sanctions Board.

***Sanctions Board*:** The Sanctions Board is the final adjudicator of contested cases. The Board is also the first non-Bank affiliated body to review the case: unlike the OSD, which is composed entirely of World Bank-appointed staff, the Sanction's Board five members are—since a revision of the Statute of the Sanctions Board in 2016—entirely external, *i.e.*, have never held a World Bank position. (Prior to the 2016 revision of the Statute, the Sanctions Board was composed of seven members, three of whom were selected from among the World Bank's senior staff by the World Bank president). The Sanctions Board reviews any allegations *de novo* on the basis of the written record before it. If requested, or if decided *sua sponte* by the Chair of the Sanctions Board, evidence may also be presented during a hearing. Final decisions made by the Sanctions Board, which describe the Board's reasoning in reaching the decision in detail, are posted on the World Bank's public website. As per the Sanctions Procedures, decisions of the Sanctions Board are non-appealable and the Sanctions Board has confirmed that it will only reconsider its decisions in narrowly defined and exceptional circumstances, such as the discovery of new and potentially decisive facts, fraud in the proceedings, and/or a clerical mistake in the original decision (Decision No. 62 ¶ 6 (January 2014); Decision No. 107 ¶ 4 (January 2018)).

2. Temporary Suspensions and Early Temporary Suspensions

When the proposed debarment exceeds a period of six months (which it does in most cases), the OSD will—at the time of the initiation of the sanctions proceedings—simultaneously impose a temporary suspension on the respondent which will remain in effect while proceedings are underway. Like debarments imposed as part of a final decision, temporary suspensions render the respondent ineligible for World Bank contracts; however, they are not announced publicly. Instead, they are posted on the

"Bank's Client Connection website" and shared only with the limited number of persons specified in the Sanctions Procedures. As a result, temporary suspensions do not trigger cross-debarment.

The OSD also has the power to issue early temporary suspensions ("ETSs") before INT has concluded its investigation. The Sanctions Procedures set a relatively low standard for the imposition of ETSs, which—given their potential to cause irreversible economic damage (before INT's investigation is even concluded)—has been criticized as a potential violation of the concerned entity's due process rights. Indeed, under the Sanctions Procedures, OSD can grant an ETS request if (i) the evidence presented by INT is sufficient to support a finding that the potential respondent has engaged in a sanctionable practice and (ii) the sanctionable practice as presented in the evidence would warrant a two-year period of debarment at a minimum. The decision to grant an ETS thus appears to depend mainly on the gravity of the underlying conduct and not on the existence of an urgent threat or imminent harm. Urgency/imminent harm, however, usually constitute *sine qua non* conditions for temporary restraining order-type mechanisms across common or civil, private or administrative systems of law.

3. Settlements and Voluntary Disclosures

In addition to contested and uncontested sanctions proceedings, INT routinely resolves investigations through negotiated resolution agreements ("NRAs"). In fiscal year 2017, INT entered into 26 NRAs (four becoming effective at the beginning of fiscal year 2018). INT and the respondent can enter into settlement discussions any time during the investigation phase and even once the proceedings have begun. Depending on the terms of the NRA, the case can be closed, sanctions reduced or proceedings merely deferred pending compliance with specified conditions, which often includes ongoing cooperation (*i.e.*, providing INT with valuable information about potential misconduct, either by the cooperating party or other companies and individuals).

High-profile NRAs reached in the past include the February 2012 settlement with French engineering firm Alstom SA and the April 2015 settlement with French global telecommunications equipment company Alcatel Lucent. More recently, NRAs of note include the December 2017 settlement with Sediver SAS, a Paris-based manufacturer of power transmission line insulators. According to the World Bank press release, Sediver SAS had made "improper payments to an employee of a consulting company to influence a tender process" in relation to the Southern Africa Power Market Project in the Democratic Republic of Congo (DRC). As part of the settlement, Sediver SAS was debarred for two years with conditional release and its parent company, Sediver SpA, was conditionally non-debarred for a period of 18 months. The sanctions represent a reduction that was credited to several mitigating factors, including the companies' payment of a financial remedy of 6.8 million euros to the DRC. Yet more recently, in April 2018, the Bank entered into a settlement with a Kenyan railroad company, Africa Railways Logistics Limited, and two related companies. The settlement is of note because Africa Railways Logistics Limited was the first company to be debarred related to an investment project funded by the International Finance Corporation (IFC), the private sector arm of the World Bank Group.

B. AfDB Sanctions Regime

The AfDB's sanctions system is currently laid out in the November 2014 AfDB sanctions procedures. Like the World Bank, the AfDB has jurisdiction to investigate and sanction five types of sanctionable practices (fraud, corruption, collusion, obstruction and coercion) committed during the

procurement or implementation of a project financed by the AfDB. Similarly, the AfDB's core proceedings are centered on one investigative body (Presidency—Integrity and Anti-Corruption ("PIAC")) and a two-tiered adjudicatory system with two distinct adjudicators (Sanctions Commissioner and Sanctions Appeals Board, respectively). Overall, the AfDB's procedures largely mirror the World Bank's sanctions regime, in part due to the MDBs' efforts to harmonize their respective anti-corruption enforcement frameworks.

Nevertheless, there are certain important variations between the two regimes. For example, the AfDB imposes a higher standard to justify imposing an early temporary suspension. The AfDB procedures specify that a request for suspension prior to the conclusion of an investigation can only be granted if the "continuous eligibility of the subject of the investigations would cause *imminent financial or reputational harm*" to the AfDB (emphasis added). In addition, under the World Bank sanctions regime, a hearing will be granted upon request as a matter of course. By contrast, the AfDB procedures indicate that the parties "have no right to an oral hearing," and any request to hold a hearing by the parties shall be granted by the Sanctions Appeals Board on a discretionary basis.

The AfDB concluded its first set of negotiated settlement agreements in early 2014 and has continued to settle with companies since then. On October 1, 2015, for example, the AfDB settled with Canadian engineering company SNC-Lavalin related to allegations of unlawful payments to public officials with respect to two AfDB-financed projects in Uganda and Mozambique. SNC-Lavalin agreed to (i) pay CAD $1.5 million to the AfDB, (ii) cooperate with the AfDB in the future, and (iii) pledge to maintain an effective group-wide compliance program, subject to review by the AfDB. In exchange, SNC-Lavalin's subsidiary which allegedly made the payments is subject to a two-year and 10 months conditional non-debarment. As discussed *infra*, the AfDB settlement represents just one of multiple, high-stake proceedings implicating SNC-Lavalin as well as several of its former executives.

In December 2015, the AfDB reached a settlement with Tokyo-based multinational conglomerate Hitachi, ending the AfDB's three-year investigation into allegations of sanctionable practices by certain Hitachi subsidiaries on a power station contract in South Africa. The settlement included the subsidiaries' debarment for one year in exchange for an undisclosed but—according to the press release—"substantial" financial contribution by Hitachi to the AfDB. Interestingly, this case is another illustration of cooperation between MDBs and national enforcement authorities. Indeed, the AfDB had shared information obtained in the course of its three-year investigation with the U.S. SEC, which, in turn, launched its own investigation into the matter. The SEC's investigation was settled in September 2015, with Hitachi agreeing to pay $19 million in civil penalties.

In May 2018, the AfDB debarred Chinese company CHINT Electric for 36 months (with an opportunity for early release after 24 months) for fraudulent practices on multiple AfDB-funded projects. According to the AfDB's announcement, in multiple bids, CHINT misrepresented its prior experience in order to meet qualification requirements. The AfDB indicated that CHINT's release from debarment is conditioned on adoption of a comprehensive integrity compliance program that meets the standards of the AfDB.

C. Other MDB Sanctions Regimes: Highlights of Recent Changes

A number of MDBs have undertaken recent changes to their respective sanctions regimes to bring them more in line with the World Bank's regime. Select highlights of such changes are presented below.

European Bank for Reconstruction and Development: Sanctions procedures at the EBRD are governed by the "Enforcement Policy and Procedures." Under these procedures, EBRD has adopted a two-tiered adjudicatory process, with an initial review by the "Enforcement Commissioner" and a second level review by an "Enforcement Committee," made up of five members (three external to the EBRD). Decision of the Enforcement Committee are final and no longer subject (as before) to the referral to the Bank's President or Executive Committee. EBRD's investigative body is the Office of the Chief Compliance Officer. The Office of the Chief Compliance Officer has the authority to bring formal sanctions proceedings or enter into negotiated resolution agreements.

Inter-American Development Bank: IADB also maintains a two-tier adjudicative system composed of the so-called "Sanctions Officer" and the "Sanctions Committee." This two-tier system is charged with resolving cases brought by the Bank's investigative body, called the "Office of Institutional Integrity." Pursuant to 2015 revisions, the Office of Institutional Integrity was given authority to enter in negotiated resolution agreements. The IADB must publish on its website all sanctions imposed by the Sanctions Officer and the Sanctions Committee. While, technically, the IADB continues to maintain discretion as to whether or not to disclose the identity of the sanctioned party or the details about the underlying misconduct, in practice, most sanctioned parties listed on the website are identified by name.

Asian Development Bank: Like the World Bank's Sanctions Procedures, the Asian Development Bank's Integrity Principles and Guidelines ("Guidelines") are built around an investigative body—the Office of Anticorruption and Integrity ("OAI")—and two adjudicative bodies (the "Integrity Oversight Committee" and the "Sanction Appeals Committee"). In order to ensure greater independence from the investigation process, the Guidelines mandate that the Sanctions Appeals Committee's chair be picked from senior ADB staff, external to the OAI. Unlike its peers, the ADB has decided not to move towards a full publication of its sanctions decisions. Instead, the ADB will continue to publish high-level (and anonymous) summaries of its sanction cases and maintains its rule that the identity of first time offenders is not publicized, unless limited exceptions apply (*e.g.,* failure to respond to notice of proceedings, failure to acknowledge debarment decision etc.). The revisions clarify the language of these exceptions. Accordingly the ADB's published sanctions list contains the names of entities and individuals who violated the sanctions while ineligible, entities and individuals who committed second and subsequent violations, debarred entities and individuals who cannot be contacted, and cross-debarred entities and individuals.

AIIB: The AIIB's sanctions process is set out in the Policy on Prohibited Practices, which was released on December 8, 2016. The AIIB's process is largely modeled on the World Bank's system, providing for a two-tiered adjudicatory system. At the first stage, the AIIB's investigative body, the Compliance, Effectiveness and Integrity Unit (CEIU), headed by a Director General, is tasked with investigating suspected misconduct. Investigations Officers look into suspicious activities and make recommendations to a Sanctions Officer, who in turn decides whether charges are supported. Respondents have an opportunity to contest the Sanctions Officer's findings before he makes a final

determination and imposes sanctions. At the second stage, respondents can appeal the Sanctions Officer's determination to the Sanctions Panel. The Panel is composed of three members, one internal and two external, who are appointed by the Bank's President. As mentioned above, in 2017, the AIIB voluntarily adopted the MDB's cross-debarment list and announced its intention to formally apply for inclusion in the MDB's Cross-Debarment Agreement.

IV. Useful Lessons from the World Bank Sanctions Board's Decisions

The World Bank has historically been the only MDB to publish the decisions of its final adjudicative body in full text. The growing body of World Bank Sanctions Board decision is of particular value, as the decisions set out, in detail, the Board's sanctioning analysis, especially with respect to the initiatives and remedial actions that it expects from companies and individuals to receive mitigating credit. These mitigation factors are discussed in every Sanctions Board decision. Of similar practical importance to many companies working on World Bank and other MDB-funded projects, the Sanctions Board has recently issued a decision, which provides a rare insight into its understanding of successorship liability.

A. Mitigation of Potential Sanctions

An analysis of published Sanctions Board decisions shows that the mitigation accorded by the Sanctions Board can indeed be meaningful. For example, in one decision, the proposed sanction of a three-year debarment with conditional release (which corresponds to the Bank's "baseline" sanction) was reduced to a six month retroactive, non-conditional debarment in large part due to a multitude of mitigating factors (Decision No. 63 ¶¶ 106-107, ¶¶ 109-110, ¶ 112 (January 2014).) The significance of mitigation credit is also evident from the increased sanctions levied when such factors are absent. (*See*, *e.g.*, Decision No. 69 ¶¶ 39, 41, 45 (June 2014).)

Below is a description of mitigating factors regularly invoked by respondents and/or used by the Sanctions Board to reduce the sanctions initially proposed. Many of these findings are consistent with decisions of regulatory agencies inside and outside the United States that have insisted on similar criteria for crediting corporate investigations of potential misconduct.

1. Cooperation with INT

The Sanctions Board will give companies and individuals mitigating credit if they cooperate during the course of the investigation conducted by INT. Interestingly, such mitigation credit can be obtained even when the company does not comply with *all* of INT's requests (Decision No. 79 ¶ 48 (August 2015), mentioning "gaps" in the company's responses to INT's queries). More noteworthy still are instances where the concerned companies were accused of initially obstructing INT's investigation. For instance, in Decision No. 60, the Sanctions Board found select respondents culpable of obstruction for having ordered the deletion of emails before INT's audit. Ultimately, however, these respondents were awarded "significant" mitigating credit for having (i) met with INT and admitted misconduct; (ii) provided inculpatory evidence and (iii) made efforts to retrieve previously deleted emails. (Decision No. 60, ¶ 133 (September 2013).) Similarly, in Case No. 63, the Sanctions Board found that attempts by a respondent entity's employees to interfere with INT's investigation warranted aggravation, while also applying mitigation for subsequent efforts by respondent entity's management to correct the employee's actions. (Decision No. 63, ¶¶ 102 and 110 (January 2014).)

Moreover, in another decision, the Sanctions Board made it clear that it will not necessarily link the mitigating credit accorded to a cooperating company to the success of the investigation conducted by INT. In this particular decision, the Sanctions Board granted mitigation to a Respondent Director who participated in two interviews with INT, despite the fact that these interviews did not shed light on an area of particular relevance to the case. Indeed, the Sanctions Board noted the lack, in the record, of any indication that INT had asked questions pertaining to these relevant areas. It would therefore appear that the responsibility for successful cooperation lies not only with the respondents but also with INT. (Decision No. 73 ¶ 48 (October 2014).)

2. Internal Investigations

Companies will also be given mitigation credit when they take the initiative to conduct their own internal investigation into the alleged misconduct. Here, it is important to note that the Sanctions Board expects (and will only give mitigating credit if) such internal investigations are undertaken by persons with sufficient independence, expertise, and experience. (Decision No. 50 ¶ 67 (May 2012).) The Sanctions Board has clarified that the burden to prove the independence of internal investigators lies with the respondents: in Decision No. 68, the Board refused to apply mitigation where a respondent had claimed that its "Board of Management" had conducted an internal investigation without specifying the composition of the Board or speaking to the independence of its members. (Decision No. 68, ¶ 43 (June 2014).)

The Sanctions Board also expects internal investigations to be adequately documented and credibly performed and that such investigations lead to concrete and targeted follow-up actions, when appropriate (for denial of mitigation on these grounds, see Decision No. 71, ¶¶ 98-100 (July 2014) and Decision No. 77, ¶ 56 (June 2015). Importantly, the Sanctions Board notes positively and accords mitigating credit when the results of an internal investigation are shared with INT and/or relevant national authorities. (Decision No. 63, ¶112 (January 2014).) However, companies sharing such information should be cognizant of the potential implications, and, in particular, of the possibility of parallel proceedings, discussed *infra*.

3. Disciplining Responsible Employees

The Sanctions Board places emphasis on disciplining responsible employees but will only provide mitigating credit if such disciplining is the result of an adequate inquiry into the matter (rather than provoked by a desire to find a convenient scapegoat). Accordingly, the Sanctions Board has declined to provide mitigation credit to companies that (i) disciplined a responsible employee without thoroughly investigating the underlying conduct to allow the company to "assess and address its own responsibility or that of other employees" (Decision No. 55 ¶ 77 (March 2013)) or (ii) did not provide any "proof of a demonstrable nexus" between the relevant employee's departure/disciplining and the sanctionable conduct at issue. (Decision No. 56 ¶ 67 (June 2013).)

Similarly, in two decisions arising out of the same World Bank–funded project, the Sanctions Board denied mitigating credit to respondents on the basis that the claimed corrective actions did not adequately target the staff actually involved in the misconduct. In one of the decisions, the respondent claimed mitigating credit for having filed a police report and terminating its relationship with the agent who had issued allegedly forged bid securities; neither of which—the Sanctions Board found—addressed

misconduct arising "within the Respondent's own staff or operations." (Decision No. 67, ¶ 39 (June 2014).) In the other decision, the respondent claimed mitigating credit for having issued a warning letter against its finance and deputy finance director. The Sanctions Board again denied mitigating credit on the basis that no disciplinary measures were taken against the marketing staff, which had allegedly processed the tender, as well as (lower-echelon) finance staff, which had processed the bid securities. (Decision No. 68 ¶ 39 (June 2014).)

4. Compliance Programs

The Sanctions Board recognizes an effective compliance program defense to vicarious corporate liability. Amidst the ongoing debate over whether there should be an "effective compliance program" defense in the context of U.S. FCPA violations, the Sanctions Board's decisions emphasize the Board's recognition of such a defense to the imposition of corporate liability for the acts of employees, under certain conditions. If an employer can demonstrate to the Sanctions Board's satisfaction that it had implemented, prior to the conduct at issue, controls reasonably sufficient to prevent or detect the conduct, the employer would appear to have a defense against liability for its employees' actions. For companies that have or may seek World Bank Group–financed contracts, these decisions create a substantial incentive to review and, as necessary, recalibrate existing compliance programs to both anticipate likely compliance risks and generally meet the World Bank's expectations for compliance programs.

The Sanctions Board also gives credit for compliance program modifications implemented in response to alleged misconduct. Even if a pre-existing compliance program had not been reasonably designed to prevent or detect the conduct at issue, the Sanctions Board has indicated that it will also provide mitigation credit for post-conduct compliance modifications designed to prevent or detect the recurrence of the alleged misconduct. (Decision No. 51 ¶¶ 51-52 (May 2012); No. 53 ¶¶ 60-61 (September 2012), No. 60 ¶¶ 129-30 (September 2013). In such cases, the Sanctions Board gives more weight to modifications that have been made prior to the issuance of the Notice of Sanctions Proceedings to respondents. (Decision No. 63, ¶ 107 (January 2014), No. 71, ¶ 94 (July 2014), No. 79, ¶¶ 46 (August 2015).)

In applying mitigation credit for the respondent's compliance program, the Board will likely examine the program's individual components, such as the company's tone at the top, the existence of a code of ethics and/or written policies on the firm's tendering guidelines, mandatory staff training, and the establishment of a comprehensive company risk assessment. (Decision No. 63 ¶ 107 (January 2014), No. 68 ¶ 40 (June 2014).) The Sanctions Board has also emphasized the importance of compliance materials and policies related to third-party due diligence. (Decision No. 78 ¶¶ 80-81 (June 2015) and Decision No. 83 ¶ 93 (September 2015).)

Limited compliance enhancements, on the other hand, lead to lesser credit. In one decision, the Sanctions Board agreed to provide "some mitigating credit, limited by the lack of more evidence" for the adoption of a company-wide prohibition against misconduct with approval and support of senior management. (Decision No. 56 ¶¶ 68-69 (June 2013).) Unit or department-level improvements can also result in some mitigation credit. (Decision No. 55 ¶ 78 (March 2013).)

B. Successor Liability

Like the procedures of most other MDBs, the World Bank's Sanctions Procedures do not define the terms "Successors" and "Assigns." Indeed, the only section dealing with "Successors and Assigns" in the Sanctions Procedures states that "any sanction imposed shall apply to the sanctioned party's successors and assigns, ***as determined by the Bank***" (emphasis added). The Sanctions Procedures simply add that "[s]uch determinations may be appealed by the party(ies) affected thereby (…)." While the absence of a formal definition of successorship in the Sanctions Procedures provides more flexibility and may thus protect the Bank from sanctions circumvention, it creates legal uncertainties for companies wishing to acquire assets or shares of an entity sanctioned by the Bank in the past.

Sanctions Board Decision No. 101 (December 2017) deals with a Successor Appeal case and thus provides a rare insight into the Bank's and the Sanctions Board's understanding of successor liability. The Sanctions Board found that the Bank had committed an abuse of discretion in determining that the "Appellant" (an information technology company) is a successor to the "Sanctioned Firm" (an entity sanctioned pursuant to two previous Sanctions Board Decisions (Decisions No. 71 (2014) and No. 87 (2016))). Such findings against the Bank are rare: indeed, the applicable abuse of discretion standard gives high deference to the Bank and is met, *inter alia*, through a showing that the Bank's determination "lacks an observable basis or is otherwise arbitrary." While the Appellant's victory in this case was largely based on the specific underlying facts as well as the—in the Sanctions Board's view—questionable evidence put forward by INT, the method used and factors considered by the Sanctions Board in making this determination is of more general interest.

First, acknowledging the absence of a formal "Successor" definition, the Sanctions Board exercised its right (granted pursuant to Section III.A, sub-paragraph 1.02(c) of the Sanctions Procedures) to consult the views of the World Bank's Legal Vice Presidency ("LEG") for "Questions as to Proper Interpretation" of the Sanctions Procedures provisions. LEG, in turn, advised that the Bank's approach to successorship is based on a concept of "economic successorship"—specifically, "whether the entity in question continues to carry out business operations of the sanctioned entity."

The Sanctions Board also took into consideration the factors set out by the Bank/INT in determining that the Appellant is a successor to the Sanctioned Firm, namely (i) common business lines and business address; (ii) ownership and managerial connections; (iii) corporate relationship (*i.e.* listing of Appellant as a company within the Sanctioned Firm); (iv) assignment of legal and financial rights and (v) public understanding/common perception that the Appellant is a successor of the Sanctioned Firm. Some of these factors were dismissed by the Sanctions Board without much analysis due to the insufficient and inadequate evidence provided by INT. Below are listed select factors, which were analyzed in greater detail and may thus serve as useful lessons to companies facing successor liability questions under the World Bank sanctions regime:

Common business lines: According to the Bank, the fact that the Sanctioned Firm and the Appellant were vendors and partners of some of the same top multinational technology companies was not strong evidence under the circumstances that the Appellant is a successor of the Sanctioned Firm. The Sanctions Board considered the realities of the underlying market and noting that—especially in the information technology market—partnering with the same global suppliers is common and thus does not *per se* provide evidence that the Applicant is a successor to the Sanctioned Firm.

Ownership and managerial connections: With respect to ownership, the Sanctions Board noted that while the Appellant had been formed in 2000 by an individual who was subsequently employed at the Sanctioned Firm between 2005 and 2013, this individual sold the Appellant in 2011, "years before World Bank sanctions were imposed on the Sanctioned Firm." The Bank determined that these circumstances did not provide "any observable basis for finding a contemporary, or even a recent, ownership connection between the Appellant and the Sanctioned Firm." As regards to managerial connections, INT attempted to provide evidence that several individuals formerly employed by the Sanctioned Firm were now in managerial positions at the Appellant. For three such individuals, the Sanctions Board directly rejected INT's claims of current employ by the Appellant based on the insufficient evidence put forward by INT, which included poorly translated media reports of "dubious" authenticity, as well as screenshots of municipal websites, the source and regular updating of which was not adequately supported. With respect to former employees of the Sanctioned Firm whose current position as managers at the Appellant were not in dispute ("Current Managers"), the Sanctions Board noted that (i) the number of Current Managers was small (four), especially when compared to the Appellant's overall manager population (41) and a total employee headcount (234); and (ii) the record did not show that the Current Managers had been senior managers at the Sanctioned Firm or otherwise involved in the misconduct that led to the sanctions. The Sanctions Board also pointed to the "highly competitive nature of the information technology sector," where the recycling of managers from one company to the next is common. Therefore, the Sanctions Board again found no observable basis for determining that the Appellant is a successor of the Sanctioned Firm.

Assignment of Legal and Financial Rights: To advance its argument for successorship, INT relied on the fact that, following the Sanctioned Firm's liquidation, the Appellant had acquired (i) one of the Sanctioned Firm's production units, and (ii) legal and financial rights under two ongoing contracts (such as trademark rights and the right to collect debt and obtain payment). The Appellant did not dispute these purchases. However, the Appellant presented evidence that the value generated by the purchased production unit and the turnover arising under the purchased contracts/rights represent only a small part of the total value of the Appellant's assets and turnover (respectively, 7% and 0.026%). The Sanctions Board gave weight to the Appellant's comparative analysis and, coupled with the absence of evidence that any of the acquired rights or assets were connected to the misconduct underlying the sanctions, determined that once again that these circumstances did not provide any "observable basis" for concluding that the Appellant was the successor of the Sanctioned Firm.

V. International Cooperation and Referrals

Companies and individuals participating in MDB-financed projects should be aware that sanctions proceedings before an MDB do not occur in a vacuum. Instead, there has been a growing trend for increased cooperation and information sharing among MDBs and between MDBs and international and national anti-corruption enforcement authorities, which can lead to parallel proceedings. Such increased cooperation is made possible through various tools. For example, according to INT's annual report for fiscal year 2017, the World Bank has signed over 55 cooperation agreements with national and international enforcement authorities (including with the UK Serious Fraud Office, the European Anti-Fraud Office, the UN Office for Internal Oversight and the International Criminal Police Organization (INTERPOL)) in support of parallel investigations, information sharing and asset recovery.

Moreover, most MDB sanctions procedures contain so-called referral clauses, which allow the MDBs in question to share information about potential sanctionable practices with other MDBs and/or international and national prosecuting authorities. In fiscal year 2017 alone, the World Bank made a total of 47 referrals to countries and other MDBs. In total, as of the end of fiscal year 2017, the Bank has made 456 referrals to anti-corruption bodies in 101 countries

As discussed below, the effects of such increased cooperation are wide-reaching, and the two-way information sharing leads to national procedures "spilling over" into MDB sanctions procedures and vice versa.

A. Referrals from National Authorities to MDBs

Information shared by national authorities can help MDBs substantiate allegations of sanctionable practices while an investigation is still ongoing. National authorities can also refer information after an investigation has been closed and the sanctions proceedings are underway. This was poignantly (and dramatically) illustrated by Sanctions Board Decision No. 72. The case underlying this 2014 decision arose in connection with two World Bank-funded projects in Iraq, for which respondents submitted successful bids with the assistance of a local agent. Among other things, INT alleged that respondents engaged in corrupt practices by offering and/or paying the agent a commission with the expectation that these funds would be used to influence procurement officials working on the projects. Respondents rejected the allegations. However, two days before the scheduled hearing before the Sanctions Board, INT obtained its evidentiary *pièce de résistance* through a referral by Iraqi national authorities, who shared with INT email correspondence in which the agent clearly stated that part of the commission would be used to make payments to a project manager. Largely based on this evidence, the Sanctions Board proceeded to debar the concerned respondents for four years, a dramatic increase from the one-year debarment with conditional release proposed by the OSD.

B. Referrals from MDBs to National Authorities

The Sanctions Board decision involving Dutch company Dutchmed BV highlights the tension that can arise between an MDB's contractual audit rights, the MDB's practice of referring matters to national authorities, and a respondent's potential rights against self-incrimination. On June 2, 2017, the World Bank Group Sanctions Board imposed a fourteen-year debarment on Dutchmed BV and its affiliates for five counts of corrupt practices and one count of obstructive practices in connection with a Bank-funded Health Sector Reform Project in Romania.

According to the decision, the respondent made corrupt payments to secure approximately $10 million worth of contracts, including illicit commissions to a procurement advisor and personal trips for personnel of a project management unit. INT also claimed that the respondent obstructed its investigations by materially impeding its audit and inspection rights and refusing access to its records. At the first tier of the sanctions regime, the Suspension and Debarment Officer found against the respondent and imposed a ten-year debarment.

The respondent appealed to the Sanctions Board, claiming that INT failed to establish the elements of corruption, and that its inability to cooperate stemmed from exercise of its right against self-incrimination under Article 6 of the European Convention on Human Rights. According to the company,

based on its status as a suspect in national criminal proceedings, compliance with INT's request for unconditional cooperation would have impaired its exercise of this privilege in future prosecutions. Given the prolific nature of the World Bank's referral practices, the fear of self-incrimination may have had some merit. As of December 2016, INT's referrals had resulted in prosecution and conviction of at least 35 individuals and criminal charges against another 29 parties.

The Sanctions Board nevertheless found against the respondent on all counts. On the obstruction charge, the Board highlighted the contractual nature of INT's audit and inspection rights, distinguishing between the Bank's administrative proceedings and criminal proceedings.

CHAPTER 6: OTHER INTERNATIONAL DEVELOPMENTS

I. E.U. Data Protection Developments

Significant developments took place in 2018 in the field of European data protection law with possible far-reaching consequences for compliance professionals. On May 25, 2018, the European Union ("E.U.") General Data Protection Regulation ("GDPR") entered into force in all E.U. Member States. The GDPR was adopted in April 2016, concluding four years of work at the E.U.-level to overhaul the E.U.'s personal data protection rules.

The GDPR's stated aims are to return control of personal data to citizens and to simplify regulations. The new set of rules enshrined in the GDPR is a modernization of the data protection regime initially established by Directive 95/46/EC, which dates from 1995. The text of the GDPR was adopted in May 2016, and gave member states two years to prepare for its entry into force. Given the importance of the GDPR, we first briefly summarize the contours of the 1995 Directive that the GDPR superseded.

Directive 95/46/EC, adopted by the European Commission on October 24, 1995 ("the 1995 Directive"), sought to protect E.U. citizens' rights with respect to their private data both when the data is used within the E.U. and when it is transferred out of the E.U. It restricted the "processing" and "transfer" of "personal data," which covers "any information relating to an identified or identifiable natural person, including workplace information pertaining to employees." The responsibility for compliance with the 1995 Directive rests on the shoulders of the "controller," meaning the natural or artificial, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Under the 1995 Directive, the "processing" of personal data covered "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." The principle was that personal data could not be processed unless three conditions were met: (i) transparency, (ii) legitimate purpose, and (iii) proportionality. Accordingly, (i) the data subject had the right to be informed when his or her personal data was being processed; (ii) personal data could only be processed for specific explicit and legitimate purposes; and (iii) personal data could be processed only insofar as it is adequate, relevant, and not excessive in relation to the purposes for which it is collected and/or further processed.

Under the 1995 Directive, the transfer of personal data was strictly prohibited when the data was intended to be transferred to non-E.U. countries, except if the recipient country provided an adequate level of protection according to the European Commission. Because only approximately a dozen non-E.U. countries are recognized as providing "adequate" protections, companies must usually rely on other grounds to transfer data outside the European Economic Area ("EEA"). Other grounds that justify such transmission of data outside the EEA include consent, necessity for the performance of an agreement, or other adequate safeguards which include standard contractual clauses issued by the E.U. Commission and intra-group Binding Corporate Rules ("BCRs").

The 1995 Directive required each EAA country to enact data protection laws that were at least as protective as the Directive itself, which led some countries to enact data protection laws more protective than the minimum required by the 1995 Directive. As a result, the degree of protection, the definition of personal data, the enforcement of sanctions, the notification requirements to Data Protection Authorities, among other things, vary from country to country within the EAA, resulting in a complex web of data privacy laws within the E.U.

To simplify this tangled web of regulation, and to strengthen online privacy rights in the modern digital landscape, the European Commission proposed in January 2012 to draft a comprehensive reform of E.U. data protection rules. This effort resulted in the 2016 GDPR.

A. The 2016 E.U. General Data Protection Regulation

The GDPR reform consists of two instruments, a Regulation and a Directive. On the one hand, the **General Data Protection Regulation** is directly applicable within the Member States and intended to enable people to better control their personal data. On the other hand, the **Data Protection Directive for the police and justice sectors** require the E.U. Member States to implement laws covering the police and criminal justice sector and ensuring that the data of victims, witnesses, and suspects of crimes are duly protected in the context of a criminal investigation or a law enforcement action.

Both the Regulation and the Directive were adopted by the European Council on April 8, 2016 and the European Parliament on April 14, 2016. The official texts of the Regulation and the Directive have been published in the E.U. Official Journal on May 4, 2016.

While the **Regulation** entered into force on May 24, 2016, it only became applicable on **May 25, 2018**. The **Directive** entered into force on May 5, 2016 and E.U. Member States had until May 6, 2018 to transpose it into their national law.

The 2016 GDPR makes numerous key changes to the 1995 Directive's regime. For example, the GDPR:

- *Creates a single set of harmonized rules on data protection, directly applicable in all E.U. Member States, to replace the complex web of existing laws*. (Directive 95/46/EC was repealed once the GDPR came into effect);

- *Introduces higher sanctions on data controllers and processors for not complying with the GDPR requirements (up to the greater of 4% of the preceding year's annual worldwide turnover of an offending organization or €20 million) and empowers each Data Protection Authority to impose "effective, proportionate and dissuasive" sanctions on a case-by-case basis*;

- *Creates a new, independent super-regulator—the European Data Protection Board ("EDPB")—that will include the head of each national Data Protection Authority and the European Data Protection Supervisor ("EDPS") or their representatives, and will replace the Article 29 Working Party (discussed below)*. The EDPB was established as a body of the European Union with a legal personality and the power to, among other functions, adopt decisions regarding disputes between national supervisory authorities, issue relevant

guidelines, recommendations, and best practices, and review the practical application of such guidelines and best practices;

- *Extends the territorial scope of the GDPR to companies outside the E.U. targeting E.U. subjects (by offering goods or services to E.U. residents or by monitoring their behavior) no matter whether the processing tool is used inside or outside the E.U.* This stands in sharp contrast to the 1995 Directive, under which the processing tool had to be located inside the E.U. to be governed by the Directive);

- *Broadens the scope of liable persons to include data processors in addition to data controllers*. Data processors will be directly liable for failure to comply with the GDPR requirements. For the first time, data processors are required to (i) maintain a record of processing activities for each controller, (ii) designate a Data Protection Officer where required, (iii) appoint an E.U.-based representative when the organization is not established in the E.U. but subject to the GDPR's long-arm jurisdictional reach, and (iv) notify the controller of all data breaches without undue delay (within 72 hours in most circumstances);

- *Broadens the definition of personal data, which now includes pseudonymized data and online identifiers.* The GDPR now specifically includes biometric data, which is defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data";

- *Introduces a principle of accountability and increases the responsibility of organizations regarding how they control and process personal data, including data governance requirements to: (i) keep extensive internal records of data protection activities; (ii) conduct Data Protection Impact Assessments for any high-risk processing activity; (iii) hire, in some large organizations, a Data Protection Officer; and (iv) notify the relevant Data Protection Authority of data breaches*;

- *Simplifies companies' interactions with Data Protection Authorities by introducing the "one-stop-shop" model*. This model allows an E.U.-based organization with a trans-European footprint to designate as its lead regulator the national Data Protection Authority of the Member State where the decisions regarding the purposes and the means of the processing are taking place. This lead regulator then coordinates with any other Concerned Authorities. It remains to be seen exactly how the one-stop-shop model will work and whether forum-shopping will emerge as a problem, it being noted that the organizations may be asked to evidence their position regarding the location of their actual decision-making center. During the EDPB's second plenary meeting in July 2018, European data protection authorities shared experiences on the functioning of the one-stop-shop mechanism and the functioning of the International Market Information System (IMIS), an IT tool used for cross-border complaints and cooperation. As of July 2018, most data protection authorities have reported a substantial increase in complaints received and about 100 cross-border cases in IMIS are under investigation;

- *Clarifies the consent required from data subjects*. Although consent could previously be assumed in certain circumstances, under the GDRP it must now be given explicitly and must be as easy to withdraw as to give, and data controllers must be able to demonstrate that consent was given;

- *Introduces provisions to ensure that profiling and automated individual decision-making (whether or not this includes profiling) are not used in ways that have an unjustified impact on individuals' rights*;

- *Increases transparency obligations within privacy notices, such that existing forms of fair processing notice will have to be re-examined*;

- *Introduces principles of privacy by design and privacy by default*. Privacy by design requires that at the early designing stages of new products, systems or technologies, organizations should implement technical and organizational measures to ensure that data protection principles are taken into account. Privacy by default requires that organizations implement appropriate technical and organizational measures for ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed.

- *Increases Data Subjects' rights to restrict certain processing and to object to the personal data being processed for direct marketing purposes*;

- *Introduces a new right to data portability,* enabling data subjects to easily transfer certain of their data from one service provider to another, and allowing individuals to receive back their personal data in a structured and commonly used and machine-readable format to be easily transferred to another data controller; and

- *Introduces a new right to be forgotten (or right of erasure),* allowing data subjects to directly require a controller to erase personal data without undue delay in certain situations, such as when consent is withdrawn and no other legal ground for processing applies or where the data is no longer required for its original purpose.

B. E.U.-U.S. Data Transfers: Safe Harbor to Privacy Shield and Umbrella Agreement

Many companies need to transfer personal data from the E.U. to the United States. Since 2000, a mechanism had been in place whereby U.S. companies could transfer E.U. personal data to the U.S. if they participated in a self-certification system known as the Safe Harbor. Then, in 2015, the European Court of Justice invalidated the Safe Harbor regime and ushered in a period of uncertainty with respect to transatlantic data transfer. In February 2016, after two years of cross-Atlantic negotiations, the European Commission issued the framework that would become the new E.U.-U.S. Privacy Shield to replace the invalidated Safe Harbor. Although the E.U. Commission endorsed the Privacy Shield in July 2016, questions remain whether the Privacy Shield will fall to legal challenge like its predecessor.

1. The E.U.-U.S. Safe-Harbor

The E.U.-U.S. Safe Harbor mechanism governed the transfers of personal data since its adequacy was recognized by the Commission in its Decision 2000/520/EC of July 20, 2000 pursuant to Article 26 of the Directive 95/46/EC (hereafter: "the Safe Harbor Decision"). In this decision, the Commission recognized that the Safe Harbor Privacy Principles issued by the U.S. Department of Commerce provided adequate protection to the citizens whose personal data was transferred from the E.U., and as a result, their personal data could be transferred from E.U. Member States to companies in the U.S. that signed up to the Principles, despite the absence of a general data protection law in the U.S. Although the Safe Harbor relied on commitments and self-certification of adhering companies, its rules were binding under U.S. law (and enforceable by the U.S. Federal Trade Commission ("FTC")) for entities that signed up to them.

The first steps toward the unraveling of the Safe Harbor Decision were taken by Edward Snowden, a former U.S. government analyst who sensationally leaked a large volume of U.S. National Security Agency files to international journalists in 2013. Among other fallout from the Snowden revelations, a European law student named Max Schrems filed suit against Facebook when he learned that, according to documents leaked by Snowden, certain American companies including Facebook were forced to share personal data—including personal data of European citizens—to U.S. intelligence agencies.

The ultimate result of the suit was the *Schrems v. Data Protection Commissioner* case in which, on October 6, 2015, the ECJ invalidated the Commission's July 2000 Safe Harbor Decision. The ECJ ruled that the Safe Harbor Decision did not contain sufficient findings on the limitations of U.S. public authorities' access to data as well as on the existence of effective legal protection against such interference. Furthermore, the Court confirmed that even where there is an adequacy decision from the Commission under the 1995 Directive, the Member States' Data Protection Authorities are required to independently examine whether data transfers to a third country comply with 1995 Directive's requirements.

2. Transitional Arrangements: Standard Contractual Clauses and Binding Corporate Rules

The invalidation of the Safe Harbor created great uncertainty in the international business community. While the Commission and the U.S. authorities had started talks on a new transatlantic data exchange agreement as early as January 2014 in the wake of the Snowden revelations, no agreement had yet been finalized at the time of *Schrems*. Thus, the question at that time was how to transfer data from the E.U. to the U.S. without the Safe Harbor. This led the Article 29 Working Party ("Article 29 WP")—the independent advisory body gathering representatives of all Member State Data Protection Authorities, the EDPS, and the European Commission—to issue a statement providing, among other things, that: (i) Data transfers can no longer be based on the Commission's invalidated Safe Harbor Decision; and (ii) Standard Contractual Clauses and Binding Corporate Rules can be relied on as a basis for data transfers until a new agreement is in place.

3. The 2016 Privacy Shield: A Safer Safe Harbor?

In a July 12, 2016 adequacy decision, the European Commission essentially approved a new Privacy Shield by recognizing that the U.S. ensures an adequate level of protection for personal data transferred under the E.U.-U.S. Privacy Shield from the E.U. to self-certified organizations in the U.S. This decision rendered the Privacy Shield Framework Principles (the "Principles") immediately applicable.

Like the now-invalid Safe Harbor, the Privacy Shield, administered by the International Trade Administration (ITA) within the U.S. Department of Commerce, rests on a system of self-certification in which U.S. organizations commit to the Principles. The Principles include several new requirements, including requirements to (i) inform individuals of data processing, (ii) maintain data integrity and purpose limitations, (iii) ensure accountability for data transferred to third parties, (iv) cooperate with the Department of Commerce, (v) ensure commitments survive as long as data is held, and (vi) ensure transparency related to enforcement actions. The Privacy Shield buttresses the role of the Department of Commerce, including giving the Department the responsibility to maintain and publicize lists of organizations participating in the Privacy Shield and monitoring and verifying that these organizations are complying with the Privacy Shield's Principles.

The Principles require U.S. companies to reply to complaints from individuals within 45 days. The Data Protection Authority will also work with the Department of Commerce and Federal Trade Commission to ensure that unresolved complaints by E.U. citizens are investigated and resolved. As last resort, an arbitration mechanism will ensure an enforceable decision.

The negotiation of the Privacy Shield resulted in the U.S. government providing strong written assurances (including representations from the U.S. Office of the Director of National Intelligence, the U.S. Secretary of State, and the U.S. DOJ, all published in the U.S. Federal Register) that any access by U.S. public authorities to personal data will be subject to clear limitations, safeguards, and oversight mechanisms. In addition, a Privacy Shield Ombudsperson, an undersecretary of the U.S. government but independent from the intelligence community, will be available to receive complaints from individuals.

Notwithstanding European concerns with respect to the alleged intrusiveness of U.S. intelligence collection activities, the final Privacy Shield includes a potentially significant caveat: "adherence to the Principles is limited to the extent necessary to meet national security, public interest, or law enforcement requirements."

On October 18, 2017, the European Commission published its report on the first annual review of the functioning of the E.U.-U.S. Privacy Shield. In this report, the Commission noted, among other things, that the U.S. authorities had implemented the necessary structures and procedures to ensure the correct functioning of the Privacy Shield. The European Commission concluded that the U.S. authorities continue to ensure an adequate level of protection for personal data transferred under the Privacy Shield and recommended several practical aspects of its framework to be improved.

Not all E.U. institutions agreed with the European Commission's position. On July 5, 2018, the European Parliament adopted a non-binding resolution on the adequacy of the protection afforded by the E.U.-U.S. Privacy Shield (2018/2645(RSP), calling for the European Commission to suspend the Privacy Shield unless the U.S. demonstrates compliance with its requirements by September, 1 2018. The

European Parliament concluded that the Privacy Shield arrangement does not provide the adequate level of protection required by E.U. data protection law and the E.U. Charter. The European Parliament evoked the recent misuse of E.U. personal data by companies certified under the Privacy Shield, such as Facebook and Cambridge Analytica, and concluded that these cases demonstrate the weakness of the Privacy Shield in ensuring the right to data protection.

Critics have charged that although the Privacy Shield is presented as being based on "notice and choice," it does not in reality give users substantial choice. While it gives companies general approval to use the personal data of any person, these persons can object only two ways. First, if an individual knows which U.S. company is using their data, then they can contact the company to actively "opt out." (Critics have also noted that the choice of an opt-out default system gives U.S. companies a significant competitive advantage over European firms that operate under the opposite presumption, with an "opt-in" system under which they must ask customers for affirmative consent.) A second method of objecting to the use of one's private data involves seeking formal legal remedy, but the rules for legal redress are not simple: a European individual who believes his or her rights have been violated would first need to contact private U.S. arbitration bodies and their European national authority, who in turn would contact the U.S. authorities, in order to ultimately address any concerns with a "privacy shield board."

Critics have also noted that the Privacy Shield does not appear to have remedied the attributes of the old Safe Harbor regime that led to its invalidation by the ECJ in the wake of the Snowden revelations. In its 2015 *Schrems* ruling invalidating the Safe Harbor, the ECJ strongly criticized mass-surveillance laws in the U.S.; not only have these mass surveillance laws not substantially changed in the meantime, but also the Privacy Shield uses the exact same wording as the Safe Harbor regarding these laws. Therefore, the new Privacy Shield may be vulnerable to the same legal arguments about permanent mass surveillance in the U.S. used to invalidate the Safe Harbor.

4. December 2016 Umbrella Agreement: a new data protection framework for criminal law enforcement cooperation

Following the European Parliament's December 1st consent, the European Council adopted on December 2, 2016, the decision authorizing the E.U. to conclude the Data Protection and Privacy Agreement (or the "Umbrella Agreement"), which puts in place a comprehensive high-level data protection framework for E.U.-U.S. law enforcement cooperation. In particular, the agreement improves E.U. citizens' rights by providing equal treatment with U.S. citizens when it comes to judicial redress rights before U.S. courts in case of privacy breaches.

The agreement establishes a set of protections that both regions are to apply to personal information exchanged for the purpose of preventing, detecting, investigating, or prosecuting criminal offenses, including terrorism. As such, it covers all personal data exchanged between police and criminal justice authorities of the E.U. member states and the U.S. federal authorities for those purposes.

The aim of the Umbrella Agreement is to facilitate criminal law enforcement cooperation while providing safeguards and guarantees of the lawfulness of data transfers. For example, those provisions include (i) clear limitations on data use, (ii) the obligation to seek prior consent before any onward transfer of data, (iii) the necessity to define appropriate retention periods, (iv) the right to access, and (v) the right to have the data rectified.

The agreement will complement existing and future E.U.-U.S. and member state-U.S. agreements between criminal law enforcement authorities. As such, it is not in itself a legal instrument for any transfer of personal information to the U.S. but it supplements, where necessary, data protection safeguards in existing and future data transfer agreements or national provisions authorizing such transfers.

The Umbrella Agreement came into force on February 1st, 2017 after the completion by U.S. authorities of their internal procedures including making the necessary designations under the Judicial Redress Act to extend the applicable protections to citizens of so-called "covered countries." To that end, the United States Attorney General designated, on January 17, 2017, the E.U. and its Member States as "covered countries." It is noteworthy that the Umbrella Agreement does not apply to three E.U. Member States – the United Kingdom, Ireland and Denmark – until and unless they decide to opt in, in compliance with Article 27. Among these three Member States, Ireland decided to join and has been accordingly also designated by the U.S. as a covered country under the Judicial Redress Act.

Finally, and as provided by the Umbrella Agreement itself (Article 23), the parties will perform a joint review of its functioning by February 2020, it being noted that the results of such examination will be made public.

5. U.S. Enforcement Actions

Approximately one year after the E.U. Commission endorsed the E.U.-U.S. Privacy Shield, the Federal Trade Commission brought its first enforcement actions against three companies. In separate complaints, the FTC brought claims against Decusoft, LLC (a human resource software developer), Tru Communication, Inc. (a printing services company), and Md7, LLC (a real estate lease manager), for falsely claiming to be certified to participate in the Privacy Shield despite never having completed the certification process. Although the cases were unrelated, each complaint pointed to the privacy policies and statements describing certain business practices made on each company's website. Ultimately, on September 8, 2017, the FTC announced that it had reached consent settlement agreements with each company. The consent agreements were subject to public comment until October 10, 2017. In July 2018, the FTC announced that ReadyTech Corporation (a California-based company which provides online training services) agreed to settle FTC allegations that it falsely claimed being in the process of certification for the E.U.- U.S. Privacy Shield.

6. The Impact of President Trump's January 25, 2017 Executive Order on the E.U.-U.S. data protection framework

On January 25, 2017, President Trump signed Executive Order 13768 entitled "Enhancing Public Safety in the Interior of the United States" (the "Order"). The Order announces an expansion of interior immigration enforcement and, in doing so, defines priorities for departments and agencies to employ all lawful means to enforce federal immigration laws and ensure the removal of persons who have no right to be in the United States. Most notably, Section 14 of the Order states that "Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."

Shortly after the Order was signed, concerns were raised about the Order's potential impact on the continued viability of the E.U.-U.S. Privacy Shield and the Umbrella Agreement. These concerns focused on Section 14, which explicitly seeks to exclude persons who are not U.S. citizens or lawful permanent residents from the protections of the Privacy Act and appears to contradict the recently enacted E.U.-U.S. data privacy agreements. Despite the alarm, though, the potential impact of the Order is likely overestimated.

Section 14 of the Order is limited in scope and provides that federal administrative agencies must ensure that their privacy policies do not extend U.S. Privacy Act protections to non-U.S. persons "to the extent consistent with applicable law." In addition to U.S. constitutional principles already providing that an executive order cannot undo or contravene an Act of Congress, the Order's deference to "applicable law" suggests that Privacy Act protections will continue to be extended to E.U. citizens through the Judicial Redress Act. Although the sentiment of the Order foreshadows the potential for future action by the Trump administration, neither the Privacy Shield nor the Umbrella Agreement should be adversely affected at this time.

The European Parliament, in its July 5, 2018 resolution, raised concerns about the consequences of Executive Order 13768 because the protections of the Privacy Act no longer apply to non-U.S. citizens. The European Parliament concluded that Executive Order 13768 does not affect the Privacy Shield, but that it indicated an intention by the U.S. executive branch to reverse guarantees and commitments regarding data privacy made to E.U. citizens during the Obama Presidency.

7. The Impact of The Cloud Act on the E.U. – U.S. data protection framework

On March, 23 2018, the Clarifying Overseas Use of Data (CLOUD) Act was enacted into law. The CLOUD Act allows U.S. law enforcement authorities to have access to data by ordering production of communication data under the Stored Communication Act (SCA) even if it is located outside the U.S. The Cloud Act also allows certain foreign countries to enter into executive agreements with the U.S., allowing foreign orders seeking access to communications data to be requested directly to U.S. service providers.

The European Parliament raised concerns regarding the Cloud Act in its resolution dated July 5, 2018, section 27, because the CLOUD Act appears to expand the ability of U.S. law enforcement to target and access people's data across international borders without making use of the mutual legal assistance treaty (MLAT) instruments. The European Parliament further indicated that the CLOUD Act could have serious implications for the E.U. as it creates a potential conflict with the EU data protection laws.

For more information, please contact:

KEVIN T. ABIKOFF
+1 (202) 721-4770
kevin.abikoff@hugheshubbard.com

LAURA N. PERKINS
+1 (202) 721-4778
laura.perkins@hugheshubbard.com

hugheshubbard.com