



**Hughes
Hubbard
& Reed**

Fall 2017

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

Attorney advertising. Readers are advised that prior results do not guarantee a similar outcome. No aspect of this advertisement has been approved by the Supreme Court of New Jersey.

© 2017 Hughes Hubbard & Reed LLP

ANTI-CORRUPTION AND INTERNAL INVESTIGATIONS PRACTICE GROUP

PARTNERS

Kevin T. Abikoff
Derek J.T. Adler
Robert B. Bell
Roel C. Campos
Sarah L. Cave
Charles W. Cohen
F. Amanda DeBusk
Melissa L. Duffy
Terence Healy
Marc Henry
Michael H. Huneke
Edward J.M. Little
Salim Saud Neto
Saud Advogados, Rio de Janeiro, Brazil
In strategic cooperation with Hughes Hubbard & Reed
Matthew R. Nicely
Neil J. Oxford
Laura N. Perkins
Elizabeth Prewitt
Bryan J. Sillaman
Nicolas Swerdloff
George A. Tsougarakis
Marc A. Weinstein
John F. Wood

COUNSEL

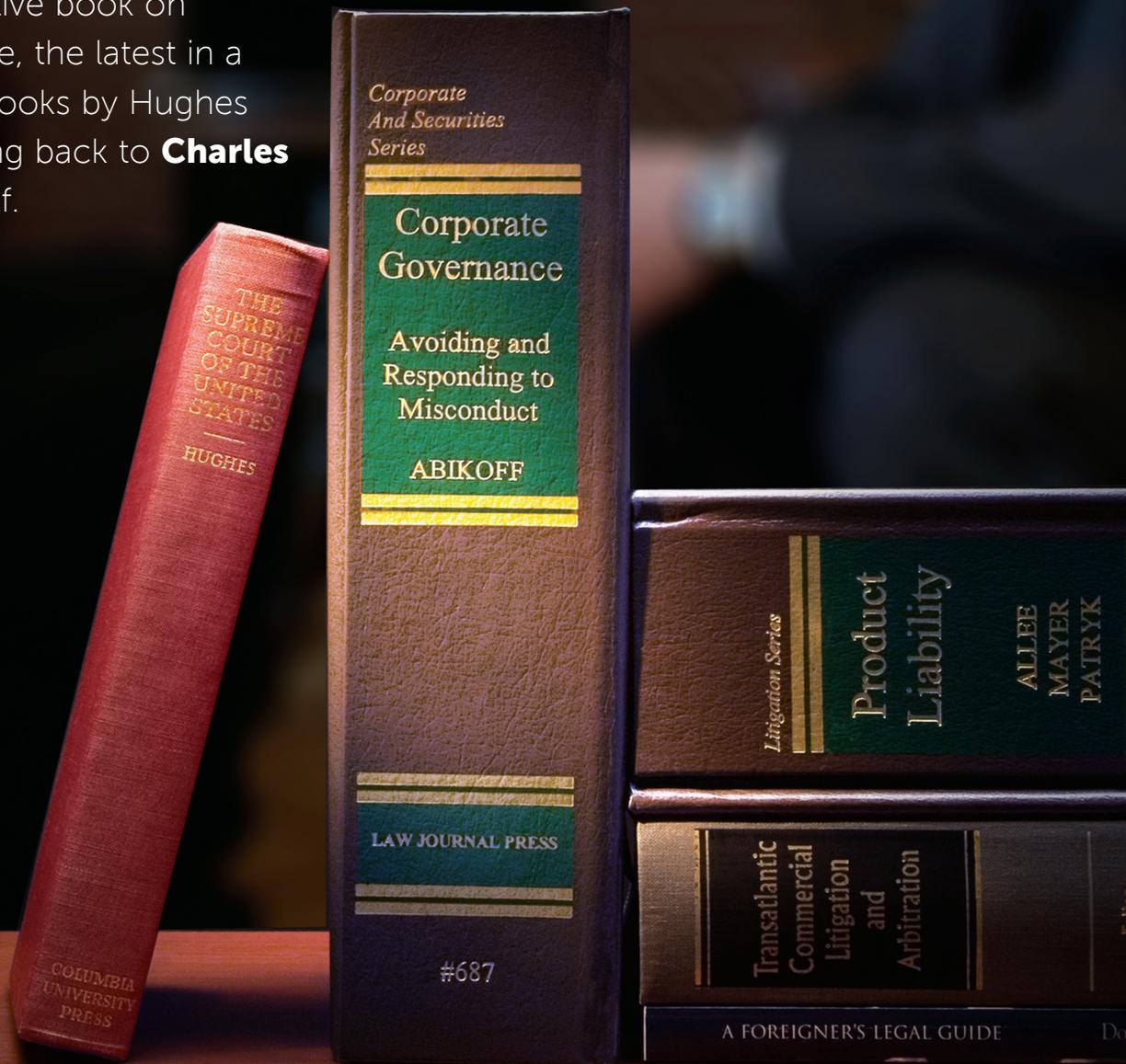
Tony Andriotis
Benjamin S. Britz
Sean C. Kane
Alan G. Kashdan
Daniel J. McLaughlin
Sean M. Reilly
Michael R. Silverman
Nicolas Tollet

ASSOCIATES & INTERNATIONAL SPECIALISTS

Ayoka Akinosi	Diogo Santana Lopes
Ernesto J. Alvarado	Katie Gerlach Merrill
Athena Arbes	Jonathan Misk
Ya'ara Z. Barnoon	Lauren E. Morris
Elizabeth A. Beitler	Robby Naoufal
Justin Ben-Asher	Marie-Agnès Nicolas
Gil Ben-Ezra	Miles Orton
Arnaldo Bernardi	N. Tien Pham
Megan Buckley	Mathilde Pardoux
Alejo R.S. Cabranes	Debbie Placid
Michael A. DeBernardis	Landon D. Reid
Jan Dunin-Wasowicz	Matthew Reynolds
Lucie Dzongang	Taylor K. Reynolds
Clémentine Foizel	Mathieu Rossignol
Stephen A. Fowler	Samuel Salyer
Anne Hukkelaas Gaustad	Sergon Sancar
Jaclyn M. Genchi	Felipe Rocha Dos Santos
Chloe Gouache	Yoshinori Sasao
Jiaxing Hao	Thomas Sisson
Ashley R. Hodges	Markus A. Stadler
Elizabeth D. Houghton	Harrison Taylor
Maureen A. Howley	Laura Vittet-Adamson
Clothilde Humbert	Vivian Wang
Adriana Ingenito	Adam Weinstein
Sigrid Jernudd	Scott Yakaitis
Robert Kolick	Mei Li Zhen
Tamara Kraljic	Jonathan Zygielbaum
Elena Linde	
Clinton T. Lipscomb	
Calvin K. Liu	

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

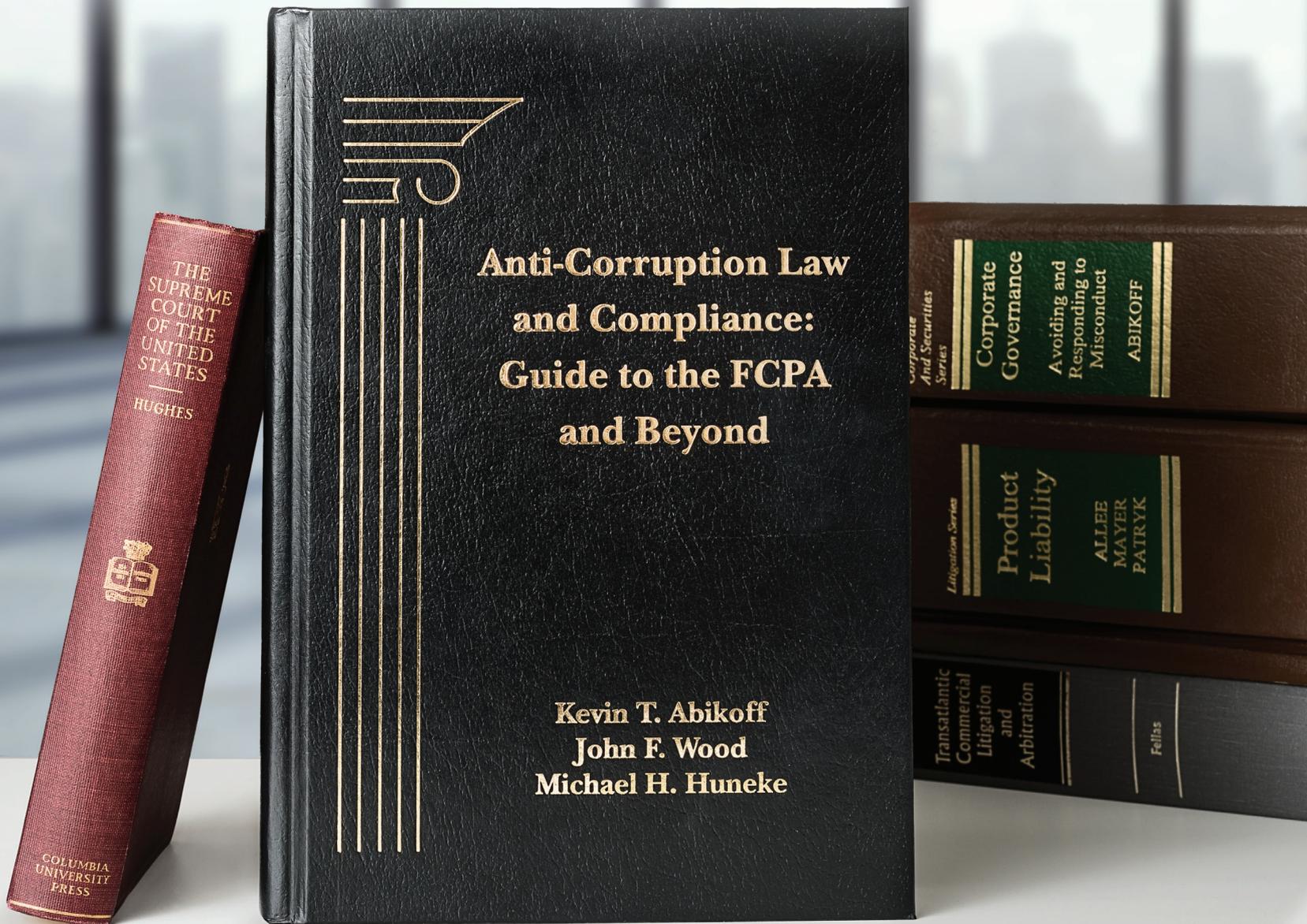
Introducing the definitive book on Corporate Governance, the latest in a distinguished line of books by Hughes Hubbard authors dating back to **Charles Evans Hughes** himself.



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



John F. Wood



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

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

John F. Wood
+1 202 721-4720
john.wood@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, Justin Ben-Asher, Gil Ben-Ezra, Megan Buckley, Benjamin S. Britz, James Canfield, Alejo Carbanes, Jan Dunin-Wasowicz, Clementine Foizel, Stephen A. Fowler, Anne Hukkelaas Gaustad, Jaclyn Genchi, Chloe Gouache, Jiaying Hao, Elizabeth D. Houghton, Clothilde Humbert, Carolyn Jackson, Robert Kolick, Tamara Kraljic, Elena Linde, Diogo Santana Lopes, Daniel J. McLaughlin, Katie Gerlach Merrill, Marie-Agnès Nicolas, Miles Orton, Landon Reid, Felipe Rocha dos Santos, Josh Rosenthal, Mathieu Rossignol, Samuel Salyer, Yoshinori Sasao, Salim Saud Neto, Michael R. Silverman, Thomas Sisson, Markus Stadler, Sydney Stringer, Jennifer Suh, Harrison Taylor, Nicolas Tollet, Laura Vittet-Adamson, Vivian Wang

INTRODUCTION

“Too Much Ain’t Enough”

*You got me on the line
Not tryin’ to call your bluff
But you just won’t be satisfied
Too much ain’t enough¹*

We are now more than a decade into what can be considered the modern era of anti-corruption enforcement, and the stakes are as high as ever. Cooperation among law enforcement around the world is leading to more thorough investigations and record-breaking settlements. In 2016 and 2017 alone, nine different companies each paid more than \$200,000,000 to resolve corruption investigations.

The U.S. continues to pace the world in its willingness to aggressively investigate and punish foreign bribery. Although President Trump, as a private citizen, famously called the FCPA a “horrible law,” there is no indication that the U.S. will change its approach to FCPA enforcement. Attorney General Sessions and other senior law enforcement officials have repeatedly asserted that the U.S. will continue aggressively prosecuting white-collar crime, including the FCPA. The DOJ and SEC announcements in September 2017 of a \$965 million global resolution with Sweden-based Telia for FCPA violations serve as a concrete indication that it will be business as usual for U.S. enforcement despite the change in administration.

Meanwhile, international advancements in anti-corruption enforcement are moving ahead at an accelerated pace. Following on the heels of the massive resolution with Rolls-Royce, the U.K. appears to be more active than ever in investigating and prosecuting violations of the U.K. Bribery Act. Brazil’s Operation Car Wash continues unabated, snaring more companies, executives, and politicians every week. With the passage of Sapin II, France is now poised to join its European counterparts, including Germany, Switzerland, Sweden, Norway, and the Netherlands, in aggressively enforcing foreign bribery laws and punishing companies for failing to implement controls to prevent such violations. The Chinese government continues its anti-corruption campaign in full force. Moreover, China’s drive to repatriate fugitive corrupt officials and their assets has led to greater law enforcement cooperation with the United States and other Western countries, a development that has potentially significant ramifications for companies doing business in China, as well as Chinese companies doing business abroad. Multilateral development banks also have growing influence in the area of anti-corruption enforcement in the developing world and continue to sanction companies for corruption and other forms of misconduct.

Companies are certainly alive to the changes in the international regulatory and enforcement environment. Responsible corporate actors have adopted robust compliance programs with increasing rigor. New and emerging technologies are allowing companies to implement better controls and monitoring, especially in connection with due diligence and auditing of third parties with whom they work. Moreover, there is no shortage of formal guidance and benchmarks against which companies can measure their programs. In just the past twelve months, the DOJ Fraud Section released guidance on evaluating corporate compliance programs and the International Organization for Standardization (“ISO”) issued the ISO 37001 Anti-Bribery Management Systems Standard.

¹ In honor of the late, great Tom Petty (1950-2017). Tom Petty & the Heartbreakers, “Too Much Ain’t Enough.” You’re Gonna Get It! LP. Shelter /ABC. 1978

But simply adding more and more controls is not always the solution. Indeed, many of the actions described in Chapter 2 of this Alert involved companies with some level of existing anti-corruption controls that proved ineffective at preventing or detecting the corrupt acts of employees. The message is clear: authorities expect companies to be vigilant in monitoring and enhancing controls to respond to ever-changing risks. Companies often mistake this message to mean *more* controls and compliance measures are needed. In reality, *better* controls and compliance measures are what is appropriate. When it comes to adopting anti-corruption compliance programs and controls, “too much ain’t enough.”

Hughes Hubbard’s Fall 2017 FCPA and Anti-Bribery Alert covers the above topics and many more. Interested parties can learn important lessons from the successes and failures of contemporaries. We hope to provide you with that opportunity in this Alert.

This Alert is divided into six chapters. Chapter 1 is devoted to analysis of certain critical enforcement trends, highlights, 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 2016 and 2017 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, Canada, China, France, and Norway. Chapter 5 provides an update related to the activities of multilateral development banks in the global fight against corruption. Finally, Chapter 6 provides updates on other international developments in the context of anti-corruption enforcement, including an update on the status of EU data protection laws and regulations.

For those so inclined, more information is included in our regularly-updated 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 2017 (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

John F. Wood
+1 202 721-4720
john.wood@hugheshubbard.com

TABLE OF CONTENTS

CHAPTER 1:	HIGHLIGHTS, TRENDS & LESSONS.....	1
I.	Enforcement Highlights and Trends.....	1
II.	Lessons from Recent Enforcement Activity	6
CHAPTER 2:	FCPA.....	10
I.	FCPA Elements and Penalties.....	10
A.	Anti-Bribery Provisions.....	10
B.	The Exception and Defenses to Alleged Anti-Bribery Violations	11
C.	Accounting Provisions.....	12
D.	Penalties	12
II.	FCPA Pilot Program.....	13
A.	Elements of Pilot Program	13
B.	Potential Credit.....	15
C.	Impact of the Pilot Program	16
D.	Recent Declinations	17
1.	HMT LLC.....	17
2.	NCH Corporation	18
3.	Linde North America Inc. and Linde Gas North America LLC	19
4.	CDM Smith.....	20
III.	FCPA Settlements and Enforcement Actions	21
A.	2017	21
1.	Halliburton	21
2.	Mondelēz International.....	23
3.	Ng Lap Seng	23
4.	Orthofix.....	24
5.	PDVSA Procurement Prosecutions: Hernandez, Ardila, and Beech	26
6.	Sociedad Química y Minera de Chile	28
7.	Mahmoud Thiam	29
8.	Telia Company AB.....	30
9.	Zimmer Biomet.....	32
B.	2016	35
1.	Anheuser Busch InBev	35
2.	Akamai Technologies.....	37
3.	Analogic, BK Medical ApS, and Lars Frost.....	39
4.	AstraZeneca.....	42
5.	Bahn, Ban, and Harris.....	43
6.	Embraer	45
7.	General Cable	48
8.	GSK.....	50
9.	Heon Cheol Chi.....	52
10.	JP Morgan Securities.....	53
11.	Johnson Controls	55
12.	Key Energy.....	57
13.	LATAM Airlines, LAN Airlines, and Ignacio Cueto Plaza	59
14.	Las Vegas Sands	62
15.	Mexico Aviation Cases.....	65
16.	Nordion and Mikhail Gourevitch.....	66
17.	Nortek.....	68
18.	Novartis	69
19.	NuSkin.....	72
20.	Och-Ziff	73

	21.	Odebrecht and Braskem	77
	22.	Olympus	81
	23.	PTC	84
	24.	PTC and Yu Kai Yuan	86
	25.	Qualcomm	87
	26.	Rolls-Royce	89
	27.	SciClone Pharmaceuticals	91
	28.	Teva Pharmaceuticals	93
	29.	VimpelCom	96
	30.	Jun Ping Zhang	100
IV.		Other FCPA Developments	102
	A.	United States Developments and Regulatory Guidance	102
		1. DOJ Compliance Guidelines	102
		2. Rulings on the Statute of Limitations in Civil Penalty Actions	103
		3. SEC Whistleblower Program	105
		4. Kleptocracy Asset Recovery Initiative	107
	B.	FCPA-Related Civil Litigation	111
CHAPTER 3:		U.K. ANTI-BRIBERY DEVELOPMENTS	121
	I.	Overview	121
	II.	U.K. Legal Privilege Considerations Relevant to Investigations	122
	III.	Recent U.K. Investigations and Enforcement Actions of Note	123
		1. Liberty Media (Formula 1)	123
		2. British American Tobacco	124
		3. Rio Tinto	124
		4. Rolls Royce	125
		5. Tesco Stores Limited and Related Individuals	125
		6. Airbus Group	126
		7. Unaoil	126
		8. F.H. Bertling Ltd and Related Individuals	128
		a. Angola	128
		b. The North Sea	128
		9. DPA with Undisclosed U.K. Company	129
		10. Peter Michael Chapman (Securrency PTY Ltd.)	130
CHAPTER 4:		ANTI-CORRUPTION ENFORCEMENT UPDATES IN SELECT COUNTRIES	132
	I.	Brazil	132
		A. Introduction	132
		B. Enforcement Highlights	132
		C. Anti-Corruption Laws	134
	II.	Canada	136
		A. Overview	136
		B. Recent Enforcement Actions	137
		1. Cryptometrics	137
		2. Griffiths Energy	139
		3. SNC-Lavalin Executives	140
	III.	China	141
		A. The Party's Inspections of State-Owned and Affiliated Entities	142
		B. International Manhunt and International Cooperation	142
		C. Creation of National Supervisory Commission	144
		D. Legislative and Regulatory Development	144
		E. First Anti-Bribery Standards for Organizations in China	145
	IV.	France	146
		A. France's History Combatting Corruption	146
		B. Sapin II	149

	C.	Other Related Legislative Initiatives.....	159
V.	Norway		162
	A.	Enforcement Focus: Yara International	162
	B.	Other Investigations and Actions of Note	165
	C.	Stakeholder Enforcement: Council on Ethics for the Government Pension Fund Global.....	167
	D.	Stakeholder Enforcement: Kommunal Landspensjonskasse	174
CHAPTER 5: MULTILATERAL DEVELOPMENT BANKS.....			175
I.	Context.....		175
II.	Why the MDB Sanction Process Matters From a Business Perspective.....		176
III.	Overview of MDB Sanctions Regimes		176
	A.	World Bank Sanctions Regime	176
	B.	AfDB Sanctions Regime	178
	C.	Other MDB Sanctions Regimes: Highlights of Recent Changes	180
IV.	Mitigation of Potential Sanctions: Useful Lessons from the World Bank Sanctions Board's Decisions.....		181
	A.	Cooperation with INT	181
	B.	Internal Investigations	182
	C.	Disciplining Responsible Employees	182
	D.	Compliance Programs	183
V.	Growing Trend of International Cooperation and Referrals		184
	A.	Referrals from National Authorities to MDBs	184
	B.	Referrals from MDBs to National Authorities	185
CHAPTER 6: OTHER INTERNATIONAL DEVELOPMENTS.....			188
I.	ISO 37001		188
	A.	Introduction	188
	B.	ISO 37001 Key Features	188
	C.	Certification by Accredited Third Parties.....	189
II.	E.U. Data Protection Developments		189
	A.	The E.U. General Data Protection Regulation.....	189
	B.	The 2016 E.U. General Data Protection Regulation.....	191
	C.	E.U.-U.S. Data Transfers: Safe Harbor to Privacy Shield and Umbrella Agreement.....	192

CHAPTER 1: HIGHLIGHTS, 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.

I. Enforcement Highlights and 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 2016 and 2017: Austria, Belgium, Brazil, Cyprus, Dominican Republic, France, Germany, Guinea, Ireland, Isle of Man, Israel, Latvia, Luxembourg, Mexico, Norway, Singapore, South Africa, Sweden, Switzerland, and Turkey.

Moreover, since the beginning of 2016, six FCPA resolutions have been coordinated with parallel resolutions by foreign governments: (i) Vimpelcom (Netherlands), (ii) Embraer (Brazil), (iii) Rolls-Royce (Brazil, U.K.), (iv) Odebrecht (Brazil, Switzerland), (v) Braskem (Brazil, Switzerland), and (vi) Telia (Netherlands). 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 but the Rolls-Royce case, 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. In the case of Rolls-Royce, the DOJ calculated a criminal penalty using the U.S. Sentencing Guidelines. Against that total penalty, the DOJ credited Rolls-Royce in an amount equal to what Rolls-Royce agreed to pay to Brazil related to the same conduct. The U.K. SFO calculated a separate penalty. Ultimately, this arrangement may have been dictated by the fact that the SFO charged Rolls-Royce for separate corrupt conduct not covered by the U.S. or Brazilian resolutions. Careful coordination of resolutions in this manner may help to ensure that a company is not double-penalized for the same conduct. Nevertheless, these global resolutions have come at a significant cost. In total these six companies agreed to pay more than *\$6 billion* in fines, disgorgement, and prejudgment interest.

- *A “Golden Age” for Massive Corporate Penalties?*: Years from now, when the dataset on FCPA settlements is sufficiently large to draw meaningful conclusions, we may all look back on the last few months of the Obama administration as a golden age for massive, jaw-dropping corporate FCPA settlements—an aberration followed by a regression to the normal pattern where nine-figure settlements are extraordinary. Or, we may look at it as a sea change, a total reset of expectations that, combined with increasingly common multijurisdictional settlements, ushered in an era where high nine-figure settlements in anti-corruption enforcement actions are commonplace. Either way, it ought to be remembered. In a three-month period from the end of September 2016 to the end of December 2016, the

DOJ and SEC entered into six separate corporate resolutions with financial penalties and disgorgement exceeding \$200 million. Embraer agreed to pay more than \$200 million to U.S. and Brazilian authorities (see p. 45). Och-Ziff (p. 73) and Teva Pharmaceuticals (p. 93) agreed to pay \$412 million and \$520 million respectively to U.S. authorities. Rolls Royce agreed to pay more than \$800 million as part of a global resolution with the U.S., U.K., and Brazilian authorities (p. 89). Braskem agreed to pay \$957 million to U.S., Brazilian, and Swiss authorities (p. 77). To top it all off, Odebrecht agreed to pay \$2.6 billion to Brazilian, Swiss and U.S. authorities (p. 77).

- *U.S. Law Enforcement Cooperation*: In addition to cooperation from foreign agencies, the U.S. DOJ and SEC credited a wide variety of domestic agencies and divisions for assistance in various of its investigations in 2016 and 2017: (i) FBI, (ii) IRS Criminal Investigation, (iii) ICE Homeland Security Investigations, (iv) U.S. Postal Inspection Services, and (v) the Federal Reserve Bank of New York. Keeping in mind that the DOJ announced in April 2016 that three new FBI squads would be dedicated to corruption, it is clear that U.S. prosecutors have vast and varied resources available to investigate foreign bribery allegations.
- *Use of Sophisticated Investigation Technology* – Cooperating witnesses, wiretaps, and sting-operations continue to play a large role in white collar investigations and prosecutions, including in the context of anti-corruption investigations. It is becoming clear, however, that regulators are using new tools as well to assist in their investigations. Recent enforcement actions show that regulators are getting more adept at using advanced computer technology to assist with large and complicated investigations. The SEC has begun using powerful technology to analyze millions of stock trades to identify potential insider trading. The U.K. SFO credited the assistance of artificial intelligence in reviewing more than 30 million documents that ultimately led to evidence of corruption by Rolls-Royce. The willingness to rely on these technologies not only may make it easier for regulators to identify potentially illicit conduct, but may free resources to pursue more investigations than in the past.
- *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 active bribery), U.S. prosecutors have successfully used money laundering laws to prosecute several foreign government officials over the past 12 months. See Heon Cheol Chi (p. 52), Mahmoud Thiam (p. 29), and PDVSA Procurement (p. 26).
- *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 2016 SQM, the Chilean company whose shares trade in the New York Stock Exchange through American Depository Receipts, settled books and records and internal controls violations with the DOJ and SEC for conduct that took place entirely within Chile (p. 28). 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 appear to be getting increasingly attenuated. For example, in the 2016 Teva Pharmaceuticals settlement, the DOJ’s only stated theory for jurisdiction over Teva’s

- Russian subsidiary was that Teva Russia employees sent emails “through the United States.” While it is far from clear whether such jurisdictional argument would be upheld if challenged in court, it appears the DOJ and SEC remain willing to extend their reach as far as companies and individuals will allow in settled matters.
- *Continued Focus on Healthcare Industry:* Pharmaceutical, health science, and medical device companies have continued to be key targets for DOJ and SEC enforcement actions. In addition to the massive \$519 million settlement with Teva (p. 93), a number of other healthcare industry companies reached settlements for violations of the FCPA and federal and state False Claims Act statutes in 2016 and 2017. These included Canadian health science company, Nordion Inc. (p. 66), U.K.-based pharmaceutical companies AstraZeneca (p. 42) and GlaxoSmithKline (p. 50), and U.S. medical device companies Zimmer Biomet Holdings Inc. (p. 32), Olympus Corp. of the Americas (p. 81), Analogic Corp. (p. 39), and Orthofix International (p. 24). In July 2017, the acting chief of the DOJ’s Criminal Fraud Section, Sandra Moser, announced that the Healthcare Fraud Unit’s Corporate Strike Force and FCPA prosecutors would start jointly investigating and prosecuting matters relating to health care bribery in the U.S. and abroad.
 - *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 13 enforcement actions in 2016 and 2017, Brazil in eight enforcement actions, Mexico in five enforcement actions, Russia in five enforcement actions, and Angola in four.
 - *Changes in Application of Disgorgement:* The DOJ and SEC have long used disgorgement to ensure that companies are not able to profit from the corrupt scheme for which they are prosecuted. Over the years, disgorgement has become a common element of FCPA resolutions. Recent policy changes and court decisions may be impacting the way in which disgorgement is used in this context.
 - *Disgorgement under the Pilot Program:* Under the DOJ’s Pilot Program announced in April 2016, to be eligible for the benefits of the Pilot Program, companies must agree to disgorge ill-gotten profits (in addition to voluntarily reporting the misconduct, cooperating with the investigation, and implementing a compliance program). This requirement for disgorgement applies even where the DOJ declines to prosecute a company under the Pilot Program. For example, in June 2017, Linde agreed to disgorge more than \$7 million in corruptly-earned profits as part of the DOJ’s decision to decline prosecution (p. 19).
 - *Disgorgement without Bribery Violations:* As an equitable remedy, disgorgement generally may be applied only when the amount can be causally connected to the violation. For this reason, disgorgement has historically been connected to anti-bribery violations, where the DOJ and SEC can determine the profit derived from the corrupt payments. However, the SEC has recently obtained disgorgement even when the company is not charged with bribery. For instance, in its settlement with Halliburton (p. 21), the SEC obtained \$14 million in disgorgement as a result of violations of the FCPA’s books and records and internal controls provisions. Similarly, the SEC obtained

more than \$2.7 million from AB InBev (p. 35) in 2016 despite not formally charging AB InBev with a violation of the anti-bribery provisions of the FCPA.

- Limitations on Disgorgement through Kokesh: In June 2017, the U.S. Supreme Court placed a significant limit on the SEC's ability to obtain disgorgement when it determined in *Kokesh v. SEC* that the five-year statute of limitations imposed by 28 U.S.C. § 2462 applies to claims for disgorgement in SEC enforcement actions (see p. 103). At the very least, this ruling could create more urgency for the SEC in finding and resolving FCPA violations. Moreover, in a key footnote in the decision, Justice Sotomayor opened a potential avenue for defendants in SEC enforcement proceedings to challenge the remedy of disgorgement altogether. Justice Sotomayor stated that nothing in the opinion should be interpreted as opining on whether courts possess the authority to order disgorgement in SEC enforcement proceedings at all, or whether the District Court had done so properly here, suggesting that courts might not possess such authority, or that such authority might at the very least need to be further circumscribed by the courts.
- Expanding Limits of Books and Records Violations: The SEC has in recent years taken an expansive view as to what constitutes "books and records" under the FCPA. This view now includes internal approval forms and compliance-related documents. For example, in its May 2015 settlement with BHP Billiton, the SEC alleged books and records violations because certain internal hospitality applications did not accurately describe the transaction. In particular, some applications described the intended SOE recipients as "customer" rather than "representative of government." Similarly, in its September 2016 resolution with NuSkin (p. 72), the SEC found that NuSkin China's characterization of a donation on an internal approval form as "charitable," when in fact it was intended to influence a party official, constituted a violation of the books and records provision of the FCPA.
- Additional Guidance on Compliance Programs: In February 2017, the DOJ Fraud Section issued its Evaluation of Corporate Compliance Programs ("Compliance Guidelines") which provides further insight into the factors that the DOJ will consider in assessing the effectiveness of a corporate compliance program as prosecutors conduct investigations, determining whether to bring charges, and negotiating plea or other agreements (see p. 102). Though the Compliance Guidelines do not materially change companies' obligations, they do provide helpful signposts for internal and external counsel and compliance officers. In the international context, in October 2016, the International Organization for Standardization ("ISO") issued the ISO 37001 Anti-Bribery Management Systems Standard reflecting international best practices for managing bribery risks and setting forth the minimum anti-bribery compliance requirements (see p. 188). Several international companies, including Wal-Mart, Microsoft, Alstom, and ENI (Italy), have announced that they have a certificate or are in the process of seeking certification.
- Emphasis on Early Cooperation: The DOJ and SEC have long signaled that extensive cooperation with their investigations may result in less severe penalties. More recently, the DOJ and SEC have shown that they consider early cooperation to be of paramount importance. The December 2016 action against Braskem (see p.77) illustrates the importance the DOJ places on early and full cooperation. While the DOJ credited Braskem

with reviewing, collecting and producing evidence located in foreign countries, analyzing and summarizing accounting records, facilitating cooperation of former employees, and providing information regarding individuals involved in the violations, it noted Braskem's cooperation did not begin until seven months after initial contact with the DOJ. In light of that delay, Braskem only received a 15% discount off of the bottom of the Sentencing Guideline penalty range, instead of the 25% discount it could have received for early and full cooperation. While an additional 10% may not seem like a significant difference, given the amounts involved, Braskem's seven month delay in cooperating may have cost it as much as \$74 million.

- *Emphasis on Self-Reporting:* For several years, the DOJ and SEC have sought to encourage companies to self-report violations, and both agencies have taken concrete actions to incentivize such reporting. In November 2015, the SEC announced a policy change, limiting the availability of NPAs and DPAs to companies that self-report violations to the SEC. In April 2016, the DOJ announced the FCPA Pilot Program, which requires prosecutors to consider declining to prosecute an FCPA violation if a company voluntarily self-reports the violation and meets certain other conditions (namely, remediation of the misconduct, cooperation with the DOJ's investigation, and disgorgement of profits earned as a result of the misconduct).

Recent enforcement actions show the impact of these policies and programs. Since April 2016, the DOJ has publicly issued declination letters to six companies under the Pilot Program. Moreover, in accordance with the Pilot Program, the DOJ has refused to give companies more than a 25% discount off of the bottom of the Sentencing Guidelines penalty range unless the violation was self-disclosed, regardless of the level of cooperation provided or remediation taken by the company. For example, in January 2017, SQM entered into a DPA with the DOJ related to corrupt payments in Chile (p. 28). After discovering the conduct in 2015 following inquiries from the Chilean tax authorities and press articles, SQM conducted an internal investigation, fired its CEO, implemented a new accounting oversight system, and reported the findings of its investigation to the DOJ and SEC. Nevertheless, the DOJ found that SQM's disclosure was not voluntary because it was prompted by an inquiry from Chilean tax authorities and press reports, and granted SQM "only" a 25% reduction off of the bottom of the Sentencing Guidelines range.

- *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. The Resource Guide notes that "[n]o executive should be above compliance . . . and no person within an organization deemed too valuable to be disciplined, if warranted." Furthermore, the DOJ has stated that "for a company to receive full cooperation credit following a self-report, it must root out the misconduct and identify the individuals responsible, even if they are senior executives."

This view has been borne out in settlement language. For example, in General Cable's settlement with the DOJ and SEC in December 2016 (p. 48), authorities noted that General Cable had fired 13 employees involved in the misconduct, three employees who had failed to provide effective supervision, and one employee who failed to report the misconduct despite becoming aware of it. General Cable, which also voluntarily-disclosed the violation, received

a 50% reduction off of the bottom of the Sentencing Guidelines penalty range and was not required to retain a compliance monitor as part of its NPA with the DOJ. 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, Embraer received a 20% discount off of the bottom of the Sentencing Guidelines penalty range, rather than the full 25% for which it was eligible. The DOJ noted that while Embraer disciplined a number of employees and executives involved in misconduct, it declined to discipline one particular executive that was aware of the bribery discussions and had oversight responsibility for the employees involved. The additional 5% could have saved Embraer as much as \$6.7 million.

II. 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. For example, if payments to an agent or others are thought to potentially be inconsistent with the FCPA, anti-corruption standards, or company policies, the initiation of an internal review or investigation is expected, and further action, such as terminating payments, disciplining or removing responsible personnel, revising internal processes and controls, revising codes of ethics and compliance training, and other similar steps, will be viewed as necessary (and favorable) by regulators. Breakdowns in internal controls should be fully remedied, and companies that encounter anti-corruption issues in one circumstance should be careful not to repeat the mistakes that led to such issues.

Identification of red flags or suspicious conduct by internal or external auditors has also been used by enforcement agencies as evidence of companies' knowledge of and failure to stop improper practices. In its 2016 settlement with Las Vegas Sands (see p.62), for example, the SEC noted that Las Vegas Sands' internal audit department had highlighted that the majority of entertainment expenses were related to entertainment of government officials, but that the auditors failed to elevate the issues sufficiently within the company. Indeed, the DOJ tends to use ignored audit findings as evidence of willfulness by companies. Similarly, in its 2017 settlement with Och-Ziff (see p.73), the DOJ noted that Och-Ziff's auditors had uncovered red flags indicating that a business partner may have been making improper payments to foreign officials, but that senior personnel had forced the auditors to remove these findings from an audit report, and had not taken any steps to address the concerns.

- *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. Nineteen of the 25 U.S. corporate settlements and prosecutions in 2016 and 2017 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 Och-Ziff settlements (see p. 73), the SEC and DOJ noted that despite operating in countries with high corruption risks, Och-Ziff conducted little to no due diligence on the third parties it engaged in those countries. These third parties ultimately engaged in widespread misconduct. In its settlement with Anheuser-Busch InBev in 2016, the SEC similarly noted that Anheuser-Busch InBev's subsidiary in India failed to conduct any due diligence on a third-party promoter who passed on reimbursements and commissions to state officials.

- *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 various shell companies, holding companies, and trusts that maintain an ownership interest in an agent or third party. The DOJ, SEC, and Public Prosecution Service of the Netherlands cases against VimpelCom Limited in 2016 (see p. 96) illustrate the risks of failing to implement a process to identify beneficial owners of third party companies. VimpelCom entered into various arrangements with a Gibraltar-based company that was ultimately owned by the daughter of the President of Uzbekistan. The arrangements were used to funnel tens of millions of dollars to the President's daughter.
- *Examine Carefully the Qualifications of Agents, Distributors, and other Third Parties:* Companies must understand the background and competence of agents and intermediaries. The DOJ and SEC criticized Nordion (see p. 66) for example, for engaging an agent that did not have any experience in the relevant 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 2016 and 2017 enforcement actions against Analogic, Mead Johnson, SAP, Olympus, Orthofix, and Zimmer Biomet 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 2016 and 2017, enforcement actions against Telia, VimpelCom, Orthofix, and PDVSA suppliers Rincon & Shiera, all involved third parties paid through agreements for non-existent 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. 21) demonstrates these difficulties and highlight's the importance of maintaining strict internal controls in the procurement context in areas where local content requirements are prevalent.
- *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 of the SEC to pursue FCPA claims even when the companies had established compliance programs at the time of the misconduct and the employees involved intentionally evaded the controls in place. Halliburton 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. In 2016, the SEC charged both SAP and Johnson Controls for failing to maintain adequate internal controls despite the fact that employees engaged in conduct specifically to evade controls. Johnson Controls maintained a system requiring any payments to vendors or third parties in China over a reasonable amount to be approved by the branch in Denmark. Employees intentionally evaded these controls in making payments to suspicious vendors by structuring the transactions in amounts just under this threshold. 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. 23). 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 2016 SEC enforcement action against Johnson Controls was based on the actions of Johnson Controls' Chinese subsidiary. Despite the fact that the subsidiary's employees actively circumvented Johnson Controls' risk-based compliance program and actively concealed improper activity from Johnson Controls, the SEC found that Johnson Controls failed to exercise sufficient oversight. Johnson Controls conducted multiple trainings and audits for its staff in China. Nevertheless, the SEC found that Johnson Controls gave too much autonomy to the local Chinese Managing Director (who organized and actively concealed the improper conduct from the parent company) and that Johnson Controls' audit procedures failed to test payments under the thresholds that were set to trigger compliance scrutiny—a weakness that was exploited by the subsidiary's employees. The Chinese affiliate had previously been owned by York International Corp., and had been one of the subjects of York's 2007 FCPA settlement. The Johnson Controls settlement indicates that the SEC may be willing to pursue enforcement actions against parent companies even when employees actively circumvent compliance policies and conceal improper activity from the parent company, particularly where high-risk subsidiaries are involved.
- *Conduct Appropriate Employee Training*: Employees overseeing high-risk transactions or operational areas (such as customs clearance and logistics) should receive frequent training. In numerous settlements, enforcement agencies have stressed that training should be conducted in languages that employees understand. In 2012, the SEC criticized Orthofix for giving anti-corruption training in English to employees who "spoke minimal English," while in 2014, the SEC criticized Bruker for failing to translate compliance materials and trainings into local languages for Chinese subsidiaries. Similarly, in the 2016 Nortek and Akamai settlements, the SEC highlighted that pre-settlement corrective steps included providing training in appropriate languages.

It is also important that companies keep records of trainings, including records of who attended the trainings. These records can be critical to a potential defense that the culpable employees were aware of company policies, procedures, and controls, and intentionally evaded those controls.

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”)² and in Title 15, United States Code,³ and (2) the Books and Records and Internal Accounting Control Provisions in Sections 13(b)(2)(A)⁴ and 13(b)(2)(B)⁵ 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,⁶ 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.⁷

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.⁸ 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.”⁹ In addition, knowledge of a circumstance can be found when there is a “high probability” of the existence of such circumstance.¹⁰ 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

² Codified at 15 U.S.C. §§ 78dd-1(a).

³ 15 U.S.C. §§ 78dd-2(a), 78dd-3(a).

⁴ Codified at 15 U.S.C. § 78m(b)(2)(A).

⁵ Codified at 15 U.S.C. § 78m(b)(2)(B).

⁶ The FCPA further prohibits payments to foreign political parties and officials thereof.

⁷ See 15 U.S.C. §§ 78dd-1(a).

⁸ 15 U.S.C. §§ 78dd-1(f)(1).

⁹ *Id.*

¹⁰ 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.¹¹

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.¹² 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.¹³ Such extended jurisdiction is not dependent upon the use of U.S. mails or means or instrumentalities of U.S. interstate commerce.¹⁴

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.¹⁵

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.¹⁶ 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.¹⁷ 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.¹⁸ 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.¹⁹ 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.

¹¹ H.R. Rep. No. 100-576, at 920 (1987) (Conf. Rep.), *reprinted in* 1988 U.S.C.C.A.N. 1547, 1953.

¹² 15 U.S.C. §§ 78dd-1(a), 78dd-2(a).

¹³ 15 U.S.C. §§ 78dd-1(g), 78dd-2(i), 78dd-3(a).

¹⁴ *Id.*

¹⁵ 15 U.S.C. §§ 78dd-1(a), (g), 78dd-2(a), (i), 78dd-3(a).

¹⁶ 15 U.S.C. §§ 78dd-1(b), 78dd-2(b), 78dd-3(b).

¹⁷ 15 U.S.C. §§ 78dd-1(f)(3)(B), 78dd-2(h)(4)(B), 78dd-3(f)(4)(B).

¹⁸ 15 U.S.C. §§ 78dd-1(c)(1), 78dd-2(c)(1), 78dd-3(c)(1).

¹⁹ 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.²⁰ 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.²¹ 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.²² 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.²³

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.²⁴ 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.²⁵ Individuals also face up to five years' imprisonment for willful violations of the Anti-Bribery violations.²⁶ Anti-bribery violations also carry civil penalties of up to \$16,000 for organizations or individuals, per violation.²⁷ These fines may not be paid by a person's employer or principal.²⁸

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.²⁹ Individuals face up to 20 years' imprisonment for willful violations of the Accounting Provisions.³⁰ Civil penalties for violations of the Accounting Provisions include disgorgement of any ill-gotten gains and

²⁰ 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.

²¹ 15 U.S.C. § 78m(b)(2)(A).

²² 15 U.S.C. § 78m(b)(2)(B).

²³ 15 U.S.C. § 78m(b)(7).

²⁴ 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).

²⁵ 18 U.S.C. § 3571(d), (e) (fine provision that supersedes FCPA-specific fine provisions).

²⁶ 15 U.S.C. §§ 78ff(c)(2)(A), 78dd-2(g)(2)(A), 78dd-3(e)(2)(A).

²⁷ 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).

²⁸ 15 U.S.C. §§ 78ff(c)(3), 78dd-2(g)(3), 78dd-3(e)(3).

²⁹ 15 U.S.C. § 78ff(a); 18 U.S.C. § 3571(d), (e).

³⁰ 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.³¹

II. FCPA Pilot Program

On April 5, 2016, in a memorandum entitled *Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance* ("Guidance"), Andrew Weissman, then-Chief of the DOJ's Fraud Section, unveiled an initiative to encourage voluntary self-reporting in FCPA cases through an FCPA enforcement pilot program ("Pilot Program"). Under the Pilot Program, companies are eligible to receive significant mitigation credit related to FCPA violations if they: (1) voluntarily self-disclose FCPA violations, (2) fully cooperate with the DOJ's ensuing investigation or follow-up questions, (3) agree to disgorge all profit earned from the illicit acts, and (4) take sufficient remedial measures, including adoption of a robust compliance program. As detailed in the Guidance, companies that take such measures are eligible for certain mitigating credit, including a reduction of up to 50% off of the otherwise-applicable U.S. Sentencing Guidelines penalty range (or a formal declination of prosecution if appropriate) and avoidance of a compliance monitor.

A. *Elements of Pilot Program*

1. Voluntary Self-Disclosure in FCPA Matters

The cornerstone of the Pilot Program 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, be made within a reasonable time of the company becoming aware of the violation, and include all relevant facts (including information regarding the individuals involved). Moreover, a disclosure is not considered voluntary if the company is required to make it by law, agreement, or contract.

The Guidance is clear that even with full cooperation and appropriate remediation, absent voluntary disclosure, 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 nothing else, this change alone is significant, as companies have in the past received greater reductions, even absent voluntary disclosure. For example, in 2014, Alcoa World Alumina LLC ("Alcoa") reached a plea agreement with the DOJ in which it agreed to pay \$209 million to resolve FCPA violations. Alcoa's penalty represented a discount of greater than 50% off of the bottom of the Federal Sentencing Guidelines fine range, despite not having voluntarily disclosed the violations. Similarly, VimpelCom's \$460 million fine to the DOJ was a 45% reduction off of the bottom of the applicable Sentencing Guideline fine range, despite having not voluntarily disclosed the misconduct prior to the DOJ's investigation. However, recent enforcement actions indicate that the Pilot Program does not preclude the Fraud Unit from offering a fine reduction for reasons other than cooperation, such as a company's inability to pay or the amount paid in fines by the company to other regulators for the same conduct. Odebrecht's \$4.5 billion penalty, for instance, already reflected the full 25% discount for which Odebrecht was eligible, but the penalty was further reduced to \$2.6 billion based on an ability-to-pay analysis, and all but \$93 million of the reduced penalty will be paid to Brazilian and Swiss regulators and credited against the \$2.6 billion total fine.

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

2. Full Cooperation in FCPA Matters

In order to be eligible for the Pilot Program, a company must also provide full cooperation to the FCPA Unit. According to the Guidance, a company must be prepared to disclose all facts relevant to the investigation, including details regarding the involvement of the company's officers, employees, or agents. Indeed, in many ways, this requirement doubles down on the 2015 Yates Memorandum, which is specifically referenced in the Guidance. In order to qualify for the Pilot Program and receive the potential mitigation offered, a company must be willing to name names.

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

- Preservation, collection and disclosure of relevant documents and information;
- Updates on the status and findings of the company's internal investigation;
- Making available for DOJ interviews any company officers or employees who possess information relevant to the investigation;
- 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;
- Disclosure of overseas documents (unless the company can establish that disclosure is legally prohibited); and
- Where requested, translation of relevant documents in foreign languages.

The Guidance 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. Moreover, the Guidance 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 pilot program, but such credit will be "markedly less" than full cooperation credit. As an example, the DOJ offered Braskem partial cooperation credit for its assistance with the DOJ's investigation of the company. Although Braskem provided evidence to the DOJ and helped to obtain the cooperation of former executives abroad, it only did so seven months after its initial contact with the DOJ, and by that point regulators had already uncovered "significant independent evidence." The DOJ offered Braskem a reduction of 15% off of the bottom end of the Sentencing Guidelines fine range, citing, among other factors, Braskem's partial cooperation in tandem with its failure to voluntarily disclose the misconduct.

3. Timely and Appropriate Remediation in FCPA Matters

A company must take appropriate and timely steps to remediate the misconduct, including implementing an effective ethics and compliance program, appropriate discipline of employees, and any other steps to reduce the risk of misconduct recurring. The Guidance is clear, however, that before even considering remediation, the Fraud Section will evaluate whether the company is eligible for cooperation

credit. A company that does not cooperate will not be eligible for credit for remedial actions, though the effect of partial cooperation remains uncertain. In its plea agreement with Braskem, discussed above, the DOJ stated that Braskem had engaged in “extensive remedial measures,” but did not specify what effect that remediation had on the final discount offered.

With respect to expectations regarding compliance programs, the Guidance acknowledges that the implementation of an effective ethics and compliance program may vary depending on the size and resources of a company. However, the Guidance 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, raising 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 the 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.

4. Disgorgement of Profit

Finally, although not classified as a formal requirement of the Pilot Program, the Guidance is clear that in order to qualify for any mitigating credit under the Pilot Program, a company will be required to disgorge all profits deriving from the FCPA misconduct. With respect to the first three declinations published by the DOJ under the Pilot Program (*see Nortek, Akamai, and Johnson Controls*), the target companies also entered into settlements with the SEC requiring the companies to disgorge their ill-gotten gains. The four declinations from the Pilot Program published since that time (*see HMT, NCH, Linde, and CDM Smith*) have required the would-be defendant companies to pay disgorgement as part of the declination itself.

B. Potential Credit

A company that meets the requirements of the Pilot Program qualifies for the full range of potential mitigation credit. In particular, companies that meet all of the requirements are eligible for up to a 50% reduction off the bottom of the U.S. Sentencing Guidelines penalty range. In addition, for companies

that meet each of the requirements, the DOJ will consider a declination of prosecution if appropriate. In making that determination, prosecutors take into account various factors including the seriousness of the offense, the profit to the company from the misconduct, and any prior resolution with the DOJ within the past five years.

Finally, the Guidance indicates that companies that qualify for mitigation credit under the Pilot Program generally are not subject to review by 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).

C. Impact of the Pilot Program

Initial commentary from the legal community on the announcement of the Pilot Program reflected skepticism regarding its impact and a belief that the Pilot Program left too much discretion to the DOJ to determine how credit should be given to participating companies. In particular, offering “up to” a 50% reduction from the bottom of the U.S. Sentencing Guidelines’ recommended penalty range provides little guarantee for companies considering self-disclosure. Shortly after the Pilot Program was announced, news leaked that the FCPA Unit had initially proposed a program that would have offered full declinations for companies that met the requirements. However, senior Justice Department leadership apparently balked at the idea of foregoing all prosecutorial discretion, and a compromise was reached.

Despite skepticism, the DOJ does appear willing to decline to prosecute companies that fully meet the requirements of the Pilot Program, at least for conduct that is neither egregious nor widespread. Since the Pilot Program was announced, the DOJ has published seven declination letters (*see 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.

It is clear, however, that a company must be willing to meet the DOJ’s expectations for cooperation if it hopes to receive full mitigating credit under the Pilot Program. In June 2016, while Nortek and Akamai were receiving declination letters for conduct that each voluntarily disclosed, BK Medical ApS (“BK Medical”) was agreeing to an NPA with the DOJ in which it was required to pay a criminal fine of \$3.4 million (*see Analogic Corporation, BK Medical ApS, and Lars Frost* for full details). Although BK Medical’s parent company, Analogic Corporation (“Analogic”), conducted an internal investigation, voluntarily disclosed the improper conduct of BK Medical, cooperated with the investigation by the DOJ and SEC, terminated or disciplined all employees involved, and enhanced its compliance program, BK Medical received “only” a 30% reduction off of the bottom of the Sentencing Guideline fine range. According to the DOJ, BK Medical was not afforded full mitigating credit because it did not disclose all relevant facts, particularly “the identities of a number of the state-owned entity end-users of the Company’s products,” and “certain statements given by employees in the course of the internal investigation.” Despite the fact that BK Medical did not receive full mitigating credit, it was not required to appoint a compliance monitor and instead received a three-year period of self-reporting regarding its compliance program.

The Pilot Program was initially intended as a one-year program, running until April 5, 2017. The month before it was set to expire, Acting Assistant Attorney General Kenneth A. Blanco announced that the DOJ would begin an evaluation of the Pilot Program's "utility and efficacy" on its official expiry date, and that the Pilot Program would "continue in full force" until the evaluation was complete. Although then-Assistant Attorney General Leslie Caldwell stated in a November 3, 2016 speech that "anecdotally [the DOJ has] seen an uptick in the number of companies coming in to voluntarily disclose FCPA violations," the DOJ has yet to release any findings from its evaluation of the Pilot Program. The ultimate success of the Pilot Program at encouraging self-reporting therefore remains to be seen.

D. Recent Declinations

1. HMT LLC

On September 29, 2016, the DOJ issued a declination letter to HMT LLC ("HMT"), a Texas-based manufacturer of storage tanks for the oil and gas industry, related to alleged violations of the FCPA's anti-bribery provisions. According to the letter, HMT earned profits of \$2,719,412 as a result of roughly \$500,000 in illicit payments to public officials in Venezuela and China. The letter required HMT to disgorge those profits as part of the DOJ's decision not to prosecute.

According to the DOJ, beginning in 2002 and carrying on until roughly 2011, HMT's sales agent in Venezuela bribed employees of Venezuela's national energy company, Petroleos de Venezuela, S.A. ("PDVSA"), and other officials to induce them to purchase HMT products. To fund this scheme, the agent would quote significantly inflated prices to PDVSA. PDVSA paid the inflated price directly to HMT, but HMT kept only the regular price of the product, remitting the difference to the agent as "commission and subcontracting fees" with the approval of HMT managerial staff in Texas. One manager became aware of the scheme at least as early as 2008, when the agent told the manager directly that he was bribing officials. Another manager obtained information sufficient to put him on notice of the scheme shortly thereafter.

In China, according to the DOJ, HMT's distributor engaged in widespread bribery of government officials from approximately 1999 through 2011. The declination letter stated, "[t]he China distributor paid bribes on almost all transactions in China." In return, the officials caused various government entities to purchase HMT's products. Although the distributor did not inform HMT of the scheme directly, the DOJ found that an HMT manager was put on notice by a series of emails from 2008-2010 detailing certain transactions.

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 HMT's:

- Timely and voluntary disclosure;
- Extensive internal investigation;
- Full cooperation, which included providing all facts it knew about the individuals connected to the schemes;
- Agreement to disgorge its ill-gotten gains;

- Ongoing enhancement of its compliance program; and
- “[f]ull remediation,” which included terminating certain employees and suspending, demoting, or freezing the bonuses of others, and terminating its relationships with the agent in Venezuela and distributor in China.

2. NCH Corporation

On September 29, 2016, the DOJ issued a declination letter to NCH Corporation (“NCH”), a Texas-based company in the industrial supply and maintenance field, and its subsidiaries in connection with alleged violations of the FCPA’s anti-bribery provisions. According to the letter, NCH’s Chinese subsidiary (“NCH China”) provided cash bribes and other items of value to Chinese public officials in order to secure sales of NCH products. NCH China allegedly provided unlawful benefits worth a total of \$44,545, earning \$335,342 in profits from the scheme. The DOJ required NCH to disgorge all profits as a condition of its decision not to prosecute.

From roughly February 2011 until the middle of 2013, employees of NCH China paid cash bribes and provided gifts, meals, and entertainment to public officials who worked at NCH China’s government-owned customers in order to persuade them to purchase NCH products. In internal accounts, NCH China recorded the expenses with descriptions such as “customer maintenance fees,” “customer cooperation fees,” and “cash to customer.” The expenses were reviewed by an executive of NCH located in the United States.

In June 2010, NCH China also provided a 10-day “business” trip to the United States and Canada for certain employees of its customers, during which only one half-day was devoted to business. NCH China paid approximately \$12,000 for non-business expenses on the trip. According to the DOJ, NCH was aware that the employees worked for a state-owned entity, that NCH China was bidding on a project for that entity while it planned the trip, and that certain expenses were not business-related. The DOJ also found that NCH “had been advised that the proposed 10-day trip might violate the FCPA.”

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 NCH’s:

- 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 or otherwise disciplining both “senior managers and lower-level employees” involved in the illegal activity, as well as upper-level executives in the United States responsible for supervising NCH China.

3. 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 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.

4. 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.

III. FCPA Settlements and Enforcement Actions³²

A. 2017³³

1. 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

³² 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.

³³ Cases and settlements have been organized alphabetically within each year.

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 of 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.

2. 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.

3. 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: 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. 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 early 2018. Ashe died of a heart attack 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 also awaits sentencing.

Ng was convicted on all six counts for which he was tried in June and July 2017. His sentencing is currently scheduled for December 2017.

4. 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.

5. PDVSA Procurement Prosecutions: Hernandez, Ardila, and Beech

In January 2017 and October 2017, three individuals pleaded guilty to various charges related to bribery schemes to influence procurement processes at Petróleos de Venezuela S.A. ("PDVSA"). The cases are a continuation of U.S. enforcement authorities' ongoing efforts to prosecute corruption related to the Venezuelan state-owned energy company.

On January 10, 2017, Juan Jose Hernandez-Comerma ("Hernandez") pleaded guilty to conspiracy to violate the FCPA and violating the FCPA in connection with his role in a scheme to bribe PDVSA officials. The same day, Charles Quintard Beech III ("Beech") pleaded guilty to conspiracy to violate the FCPA for participating in a separate scheme to bribe PDVSA officials. On October 11, 2017, Fernando Ardila Rueda ("Ardila") pleaded guilty to conspiracy to violate the FCPA and violating the FCPA for his role in a scheme to bribe PDVSA officials that involved many of the same conspirators as the case against Hernandez.

Between December 2015 and January 2016, the DOJ prosecuted six individuals for their roles in bribery related to PDVSA (see "PDVSA Procurement Prosecutions: Rincon, Shiera, & Millan, and Ramos, Gravina, & Maldonado," FCPA and Anti-Bribery Compendium). Three of the individuals prosecuted were bribe payers, while the other three were former PDVSA officials who received bribes. In the earlier cases, the DOJ accused Roberto Enrique Rincon Fernandez ("Rincon"), Abraham Jose Shiera Bastida ("Shiera") and Moises Abraham Millan Escobar ("Millan") of engaging in a long-running scheme to bribe PDVSA officials to win contracts and otherwise receive favorable treatment in the award of procurement contracts. Shiera, based in Florida, and Rincon, based in Texas, operated competing companies that supplied goods and services to PDVSA. From approximately 2009 until 2014 Shiera and Rincon engaged in a coordinated effort to bribe PDVSA officials to win various supply contracts. Millan was a former employee of Shiera, and acted as an agent of both Shiera and Rincon's companies in connection with the bribery scheme. Shiera and Rincon pleaded guilty to conspiracy to violate the FCPA and violating the FCPA, while Millan pleaded guilty to conspiracy to violate the FCPA.

The DOJ also charged former PDVSA employees Jose Luis Ramos Castillo ("Ramos"), Christian Javier Maldonado Barillas ("Maldonado"), and Alfonzo Eliezer Gravina Munoz ("Gravina") in connection

with the scheme. The bribe receivers all pleaded guilty to conspiracy to commit money laundering. Sentencing for all defendants is set for February 8, 2018.

a. Juan Jose Hernandez Comerma

Hernandez was the general manager and partial owner of one of Shiera's companies. From approximately 2008 and until 2012, Hernandez participated in the conspiracy to bribe PDVSA officials along with Shiera, Rincon, and Millan. In particular, Hernandez was involved in bribing Gravina and a second, unnamed official, who was a purchasing analyst and who has now also been charged in a case that is, as of the date of writing, still under seal. Hernandez specifically acknowledged participating in conversations regarding the scheme, soliciting and agreeing with officials that Shiera and Rincon's companies would pay them bribes, causing bribe payments to be wired to PDVSA officials and their relatives, and providing PDVSA officials with things of value, including recreational travel, meals, and entertainment.

b. Fernando Ardila Rueda

Ardila was a sales director and partial owner of several of Shiera's companies who had specific responsibility for approaching and developing relationships with PDVSA officials to generate business. From approximately 2008 until 2014, Ardila participated in the conspiracy to bribe PDVSA officials along with Shiera and Rincon. Like Hernandez, Ardila specifically acknowledged participating in conversations regarding the scheme, soliciting and agreeing with officials that Shiera and Rincon's companies would pay them bribes, causing bribe payments to be wired to PDVSA officials and their relatives, and providing PDVSA officials with things of value, including meals and entertainment. According to charging documents, Ardila frequently circulated a series of spreadsheets to his co-conspirators that tracked the bribe payments owed to various PDVSA officials who were identified by nicknames and numbers. Ardila generally referred to the spreadsheets as "Schindler's List."

c. Charles Quintard Beech III

Beech is a Texas businessman who owns and controls a number of companies that provided services to PDVSA. From approximately 2011 until 2012, Beech conspired to bribe PDVSA officials, including Gravina and another unnamed PDVSA official. Beech admitted to wiring bribe payments to relatives of the PDVSA officials and other designated entities, including to a U.S. bank account. In return, these PDVSA officials were expected to assist Beech's companies win PDVSA purchase orders, provide Beech with inside information concerning PDVSA bidding processes, place Beech's companies on certain bidding panels for PDVSA projects, and help Beech's companies receive payment for previously awarded PDVSA contracts. Amongst other things, the charging documents note that in August 2012, Beech caused \$132,240.32 to be wired from a U.S. bank account of one of his companies to a Swiss bank account of a company controlled by the unnamed official. In return, the official helped give payment priority to Beech's companies ahead of other PDVSA vendors with outstanding invoices. The use of a Swiss bank account may explain why the DOJ's press release announcing the charges against Beech and Hernandez, like the earlier announcement regarding Rincon, notes that the Swiss Federal Office of Justice provided assistance in connection with these cases.

6. 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.

7. 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.

8. 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 p. 96).

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 up-front 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.

9. 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 follow-up 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.

B. 2016

1. Anheuser Busch InBev

On September 28, 2016, the SEC issued a cease-and-desist order against Anheuser-Busch InBev ("AB InBev") as part of a settlement with AB InBev related to violations of the FCPA's books and records and internal controls provisions, as well as the Exchange Act's Rule 21F-17(a) whistleblower protection provision. AB InBev is a global brewing company based in Belgium with American Depository Shares traded on the New York Stock Exchange. As part of the settlement, AB InBev agreed to pay the SEC \$6,008,291, including a disgorgement of \$2,712,955, a civil penalty of \$3,002,955 and prejudgment

interest of \$292,381. AB InBev also agreed to self-report on the operation of its FCPA and anti-corruption compliance program for a period of two years.

The following facts are derived from the SEC's cease-and-desist order. AB InBev neither admitted nor denied these facts.

a. Books and Records and Internal Control Violations

The SEC's findings relate to AB InBev's manufacturing and distribution operations in India between 2009 and 2012. AB InBev ran its Indian operations and beer production through its wholly-owned Indian subsidiary, Crown Beers India Private Limited ("Crown"). Crown, for its part, marketed and distributed its beer through InBev India International Private Limited ("IIPL"), a joint venture between AB InBev and RJ Corp Ltd. (an Indian corporation).

In 2009, IIPL engaged a third-party promoter – referred to as "Promoter Company A" in the SEC's order – to handle the marketing, distribution, and promotion of Crown beer in the Indian state of Andhra Pradesh. IIPL and Crown failed to conduct any due diligence on Promoter Company A. IIPL and Crown also failed to execute a contract with Promoter Company A. Between 2009 and 2012, IIPL paid Promoter Company A unsubstantiated and above-market reimbursements and commissions, the excess of which were diverted towards state officials in Andhra Pradesh. IIPL then passed along these reimbursement and commission costs to Crown, which recorded them as legitimate business costs.

In 2011, IIPL retained "Promoter Company B." Promoter Company B had no experience in the industry and appeared to be engaged solely for its connections to high-ranking local officials. While IIPL and Crown ostensibly performed due diligence on Promoter Company B, such due diligence was not performed until well after Promoter Company B had provided services and been compensated. Moreover, IIPL unilaterally amended Promoter Company B's initial responses to the due diligence forms and then backdated the forms to make it look as though they had been completed prior to Promoter Company B's engagement. IIPL also backdated a contract with Promoter Company B to make it look as though the contract had been entered in April 2011 (when Promoter Company B was first engaged). According to the SEC, the contract was not actually executed until January 2012.

Promoter Company B ultimately secured additional beer brewing hours for Crown from the local Indian authorities. In order to break into Tamil Nadu's beer market, IIPL also hired Promoter Company B to elicit beer orders from the state authority. In connection with these sales, Promoter Company B billed IIPL (and Crown) for inflated and unsubstantiated commissions, which the Company used to make improper payments to Tamil Nadu officials.

AB InBev received a series of internal complaints in 2009, 2010, and 2011 regarding the questionable use of third-party promoters by IIPL. In December 2009, an internal complaint was lodged with AB InBev regarding potential FCPA issues with Promoter Company A. As a result, AB InBev expedited an already planned audit of IIPL in 2010. The audit identified certain deficiencies in controls at IIPL, but did not scrutinize Promoter Company A's activities and thus failed to offer any findings or recommended remediation with respect to promoter Company A. IIPL continued to engage Promoter Company A until 2012.

b. Whistleblower Violations

In 2010 and 2011, a Crown employee reported concerns regarding potential improper payments by Promoter Company A and Promoter Company B's questionable business model to AB InBev management. In 2012, the employee was terminated. Following mediation regarding potential employment law claims related to his termination, the (now former) Crown employee signed a "Confidential Agreement and General Release" (referred to as "Separation Agreement" by the SEC).

The Separation Agreement threatened liquidated damages of \$250,000 in the event the Crown employee disclosed "any and all unique, confidential and/or proprietary information and material belonging or relating to [the AB InBev subsidiary]." According to the SEC, AB InBev had frequently used similar language and the threat of liquidated damages in other employment termination agreements.

Prior to signing the Separation Agreement, the Crown employee had been cooperating with the SEC in its investigation into the activities of Crown and IIIPL in India. The Crown employee stopped cooperating after signing the Separation Agreement. Based on the language in the Separation Agreement, the Crown employee believed that he would be liable for the liquidated damages if he continued to cooperate with the SEC. The SEC ultimately had to issue an administrative subpoena before the Crown employee would resume communicating with the SEC. The SEC found that the Separation Agreement's language "impeded the Crown employee from communicating directly with the Commission staff" about possible securities law violations, in violation of Rule 21F-17(a).

c. Remediation

In 2015, AB InBev dissolved IIIPL and consolidated its Indian operations at Crown. AB InBev also conducted extensive FCPA training for Crown personnel and implemented enhanced compliance policies and controls at Crown. The reorganization also included appointing a dedicated India compliance manager.

In 2015, AB InBev also amended its Separation Agreement to include permissive language regarding disclosures to government agencies. As part of its settlement with the SEC, AB InBev agreed to take steps to contact certain former employees of its U.S. operations previously identified by the SEC and inform them that AB InBev does not prohibit former employees from contacting the SEC regarding possible violations of federal law or regulation.

2. Akamai Technologies

On June 6, 2016, the DOJ issued a declination letter regarding its investigation of Akamai Technologies, Inc. ("Akamai"), a NASDAQ-listed, Massachusetts-based technology provider of cloud computing services. The following day, the SEC announced that it entered into a Non-Prosecution Agreement ("NPA") with Akamai with respect to related allegations that the company's wholly-owned subsidiary, Akamai (Beijing) Technologies, Co. Ltd ("Akamai-China"), had paid bribes to government officials in China between 2013 and 2015. These payments were masked as legitimate transactions, causing Akamai's consolidated accounts to be inaccurate. In addition to its obligation to cooperate with the SEC, Akamai agreed to pay \$671,885, including \$652,452 in disgorgement and \$19,433 in prejudgment interest.

a. Non-Prosecution Agreement with the SEC

According to the SEC, Akamai failed to maintain accurate books and records and to devise and maintain a system of internal controls that would have reasonably prevented and detected improper payments made by Akamai-China to Chinese government officials. According to the NPA, the following findings would have been proven as facts if the case had been taken to trial, and Akamai agreed in the NPA not to dispute, contest, or contradict these findings in the event that it violates the NPA and is later prosecuted on the basis of these findings.

The SEC described two types of bribe payments: improper gifts and entertainment that Akamai-China gave directly to end users (some of whom were Chinese public officials), and money and things of value given by a Regional Sales Manager working together with a local Chinese intermediary to end users (some of whom were Chinese public officials). Akamai-China used these bribes to induce end users to purchase 100 times more network capacity than they needed.

From at least 2013 to at least 2015, Akamai-China's Regional Sales Manager collected kickbacks from a local intermediary and used part of the money to bribe three end users of Akamai-China services, two of whom were state-owned entities. According to the SEC, Akamai-China was required by Chinese regulation to distribute its cloud computing services in China through intermediaries called Channel Partners, and one of these Channel Partners entered into the scheme to pay kickbacks to Akamai-China's Regional Sales Manager. According to the SEC, the Channel Partner paid money into the Regional Sales Manager's bank account, or the accounts of his nominees, and the Regional Sales Manager "then paid a portion of these funds, and also provided expensive gifts, to employees of the three end customers." These payments or gifts were worth approximately \$155,500, of which approximately \$38,500 was paid in cash to government officials. Akamai-China was also cited as having directly given approximately \$32,000 worth of gifts and entertainment to end user employees during the same period.

i. *Lack of Internal Accounting Controls and Inaccurate Books & Records*

The SEC found that Akamai's control failures at Akamai-China enabled the bribery to go undetected. Among others, Akamai failed to devise and maintain (i) a system of internal controls that would have reasonably assured that transactions were executed in accordance with the company's policies and were accounted for, (ii) a formal due diligence process for its Chinese partners, (iii) procedures for effectively reviewing and approving gifts and entertainment, and (iv) a process for monitoring or reviewing customer usage in high risk regions. Akamai also failed to exercise its audit rights to ensure compliance with anti-bribery policies, to provide adequate employee training on anti-bribery policies, and to translate compliance policies into Mandarin.

ii. *Self-Reporting, Cooperation, and Remedial Measures*

Akamai promptly self-reported to the SEC and DOJ and conducted a thorough investigation upon receipt of a December 2014 whistleblower complaint from an Akamai-China sales representative that the Regional Sales Manager had received improper payments from Channel Partners and had made improper payments to end users to obtain business. We note that the time period between whistleblower complaint and the SEC NPA (and DOJ Declination) was approximately 18 months.

The SEC acknowledged Akamai's cooperation and remedial steps. In addition to its self-reporting, Akamai provided detailed findings of its internal investigations, including results of audits of its Chinese partners, summaries of witness interviews, and factual chronologies with supporting documentation. Akamai also identified and presented relevant documents to the SEC, along with timely updates of information and progress on remedial measures, provided translated documents, and made witnesses available for interviews and testimony.

The SEC identified several concrete remedial steps taken by the company. The Regional Sales Manager was placed on administrative leave, and subsequently resigned in April 2015. Akamai also terminated the relationship with the culpable local partner. Further, the company conducted a comprehensive global review of its compliance program, and initiated steps to ensure its employees were receiving adequate training. Among other actions, Akamai (i) implemented a comprehensive due diligence process for its partners, and engaged an external consultant to conduct risk assessments, (ii) strengthened its anti-corruption policies, (iii) enhanced its monitoring functions, including naming a Chief Compliance Officer and a global team of compliance professionals, (iv) provided extensive mandatory trainings on the FCPA and anti-corruption policies in appropriate languages, and (v) enhanced its travel and expense control requirements in China.

b. DOJ Declination

The DOJ declination letter, publicly released by Akamai, cited the FCPA Pilot Program as basis for according Akamai credit for its voluntary disclosure of misconduct by an Akamai-China employee and a local Chinese service distribution partner. As factors contributing to the declination decision, the DOJ noted Akamai's full disgorgement of ill-gotten gains to the SEC, its full cooperation with the DOJ (which included identification of relevant individuals and agreement to continue cooperating with any individual prosecutions), and the steps taken to enhance its compliance program and internal accounting controls. The DOJ cited remedial measures including the prompt suspension of an employee involved in the misconduct (and that individual's subsequent resignation), the disciplining of five other involved employees, and the termination of the Chinese service distribution partner.

3. Analogic, BK Medical ApS, and Lars Frost

On June 21, 2016, NASDAQ-listed Analogic Corporation ("Analogic") and its wholly-owned Danish subsidiary, BK Medical ApS ("BK Medical") agreed to pay nearly \$15 million in criminal penalties and disgorgement to settle DOJ and SEC charges of violating the FCPA's books and records and internal controls provisions. Specifically, subsidiary BK Medical entered into a Non-Prosecution Agreement with the DOJ which included a \$3.402 million penalty, three years of reporting to the DOJ, and a commitment to cooperate with any related U.S. or foreign authorities' investigations or prosecutions, including of related individuals. The SEC settlement involved only Analogic and the former CFO of its subsidiary, BK Medical. The SEC did not require Analogic to pay a civil penalty, but did require Analogic to pay \$7.673 million in disgorgement plus \$3.81 million in pre-judgment interest. The SEC required BK Medical's former CFO, Danish-resident Lars Frost, to pay \$20,000 to resolve charges, which he neither admitted nor denied, that he violated the books and records and internal controls provisions of the FCPA.

a. Distributors Directed BK Medical to Make Bribe Payments

Massachusetts-based Analogic manufactures and sells health care technology, and its subsidiary BK Medical focuses on ultrasound equipment. During the relevant time, BK Medical sold its equipment either directly or through distributors in various countries, including Russia, where BK Medical sold equipment exclusively through unnamed “Distributor 1” to hospitals or medical facilities that were either owned or controlled by Russia and that “performed functions that the Russian government treated as its own, and thus were instrumentalities of the Russian government” for the purposes of the FCPA.

At the heart of the settlement are charges that BK Medical engaged in over two hundred sham transactions involving distributors between 2001 and 2011, funneling approximately \$20 million to third parties. The DOJ stated that BK Medical paid approximately 80% of these bribes, or approximately \$16 million, on the instructions of Distributor 1 in Russia. Although the majority of details in the settlement were provided with respect to Distributor 1 in Russia, the SEC noted that some of BK Medical’s hundreds of suspicious payments were also made through distributors working in Ghana, Israel, Kazakhstan, Ukraine, and Vietnam.

In its relationship with Distributor 1 in Russia, BK Medical kept two sets of invoices for each sale: the correct invoice, and the inflated “special” invoice. According to the DOJ, after BK Medical sent Distributor 1 the correct invoice for each sale, Distributor 1 would request that BK Medical provide a second, inflated fictitious invoice outside of the normal invoicing and accounting system. According to the SEC, BK Medical personnel created the second, fictitious invoice by cutting and pasting the BK Medical logo and other elements onto the template sent by Distributor 1 in order to create this document outside of the normal invoicing system. In 2004, a BK Medical Senior Vice President of Sales for distributors provided Distributor 1 with the following draft text to include in the second, fictitious invoice that would be sent back to BK Medical as a way to explain the overpayment:

Please note that this is simply a part of the Russian market conditions and it is a result of our process going from the former Soviet planning economy . . . the level of official salaries in many sectors are extremely low which makes it impossible to maintain a reasonable standard of living. The money we request you to transfer are not in any way money for [Distributor 1], you already know about this, but is is [sic] for various obligations that is [sic] not in our control. We know that sometimes that money goes back into the regions for education and training, which under normal conditions would not be possible, but also for general improvement of the living standard among a lot of different persons, not only persons on high levels . . . If you cannot continue to help us with the money transfers, we will risk up to 90% of our B-K business . . . Please understand that your Western word 'bribe' is not used in our Russian market. . . .

Distributor 1 would pay BK Medical the inflated price shown on the fictitious invoice, but BK Medical would only record the real price as revenue while crediting the excess amount to its accounts receivable account for the Russian distributor—essentially creating a slush fund—until BK Medical received further instructions from Distributor 1.

At some point after the overpayment, Distributor 1 would instruct BK Medical to pay the excess funds to unknown third parties, both individuals and entities including shell companies. None of the recipients of these payments had any business relationship with BK Medical, and BK Medical did not conduct due diligence on any of the recipients, but instead “merely sent them money” at the direction of Distributor 1. According to the SEC, the recipients “ranged from apparent shell corporations located in places such as Belize, the British Virgin Islands, Cyprus, and Seychelles, to specific individuals in Russia.” According to the DOJ, “there is evidence that at least some of these payments to third parties were ultimately [made] to doctors employed by Russian state-owned entities.” The SEC stated that approximately half of the payments related to Distributor 1 were made to banks in Latvia, on Russia’s border.

On certain occasions, Distributor 1 provided false invoices from certain unknown recipients that indicated that the recipients had provided “marketing” or “logistic services” or services for which a “commission” was owed, but BK Medical employees confirmed that none of the recipients provided any services to BK Medical. Finally, because the payments were made from the excess funds in the accounts receivable system, they circumvented the normal vendor approval process for payments made from the accounts payable system.

The SEC also noted that, while the above methodology was followed for the majority of the suspicious payments, on at least two occasions BK Medical made direct payments to unknown recipients in advance of the sale through, and payment from, Distributor 1. According to the SEC, BK Medical paid “approximately \$95,000 in total payments to unknown third parties, for unknown reasons, before receiving the [corresponding] funds from the Russian distributor.”

b. A Missed Opportunity in 2008

In 2008, an Analogic Senior Vice President identified the risk of bribery in BK Medical’s business, and recommended that BK Medical implement an FCPA training program and an “official process for validating that their distribution partners do not, or are not likely to engage in prohibited behavior.” While Analogic did provide FCPA training to BK Medical sales and finance staff, “no official process was implemented, and no steps were taken to validate whether [Distributor 1 in Russia] or any other distributor was engaged in prohibited behavior.”

c. DOJ Pilot Program: Incomplete Cooperation & Partial Credit

When Analogic discovered the payment arrangements at BK Medical in 2011, Analogic (1) halted the transactions; (2) conducted an internal investigation; (3) self-reported its findings including a full accounting of all suspicious payments to third parties by distributor and recipient; (4) cooperated with the SEC’s investigation and cooperated partially with the DOJ’s investigation; (5) terminated eight BK Medical distributors; (6) improved BK Medical’s distributor due diligence; (7) terminated BK Medical employees including former CFO Lars Frost and the Senior Vice President of Sales for distributors; (8) disciplined other BK Medical employees related to the suspicious transactions; (9) enhanced Analogic’s oversight of BK Medical including BK Medical’s hiring of a compliance officer; (10) improved BK Medical’s internal accounting controls; and (11) required additional and ongoing compliance training for relevant employees.

BK Medical’s NPA is the DOJ’s first corporate enforcement action under the DOJ pilot program announced early April 2016, which promotes voluntary self-disclosures, cooperation, and remediation.

The DOJ noted that although BK Medical had self-disclosed and engaged in extensive remediation, BK Medical did not receive full credit for its cooperation because its “cooperation subsequent to its self-disclosure did not include disclosure of all relevant facts that it learned during the course of its internal investigation; specifically, the Company did not disclose information that was known to the Company and Analogic about the identities of a number of the state-owned entity end-users of the Company’s products, and about certain statements given by employees in the course of the internal investigation.”

Under the parameters of the DOJ’s pilot program, the DOJ can offer a company up to 50% reduction below the U.S. Sentencing Guidelines fine range (up to 25% for full cooperation without self-disclosure, and up to 50% for self-disclosure followed by full cooperation). The DOJ stated that BK Medical received full credit for self-disclosure available under the DOJ Pilot Program, but did not specify the breakdown of credit given for disclosure and remediation. In total, BK Medical received a 30% discount off the bottom of the U.S. Sentencing Guidelines fine range.

d. SEC Settlement with Former BK Medical CFO Lars Frost

Lars Frost, who worked in BK Medical’s finance department beginning in 1999 and served as its CFO from 2008 until his termination in September 2011, agreed to pay a civil penalty of \$20,000 to settle SEC allegations that he knowingly circumvented BK Medical’s internal controls and falsified its books and records.

The SEC found that Mr. Frost personally authorized around 150 improper payments to unknown third parties, ten of which were authorized during his tenure as CFO, knowing that such payments violated and circumvented the internal accounting controls of the company. According to the SEC, both before and after he became CFO, Mr. Frost submitted false quarterly sub-certifications to Analogic certifying the company’s compliance with internal accounting controls. The SEC further alleged that Mr. Frost was also aware of the fake contracts requested by Distributor 1 and failed to disclose them despite his responsibility of completing quarterly checklists designed to identify unusual transactions for Analogic’s controller. Because the false elements were incorporated into Analogic’s books and records, the SEC found that “Frost was a cause of Analogic’s [FCPA] violations.”

4. AstraZeneca

On August 30, 2016, the SEC entered a cease-and-desist order (“Order”) against AstraZeneca PLC (“AZN”), a London-based global biopharmaceutical corporation, in connection with allegations that AZN’s wholly-owned subsidiaries in China and Russia violated the FCPA’s books and records and internal controls provisions. Without admitting or denying the SEC’s findings, AZN agreed to pay \$4.325 million in disgorgement, \$822,000 in prejudgment interest, and \$375,000 in civil penalties. After a lengthy investigation, the DOJ declined to prosecute the conduct.

a. Alleged Misconduct

According to the SEC, between 2007 and 2010, AstraZeneca (Wuxi) Trading Co. Limited (“AZ China”) made corrupt payments to health care providers (“HCPs”) employed at state-owned or state-controlled hospitals in China to incentivize the purchase and prescription of AZN drugs. According to the Order, AZ China employees submitted fake *fa piao* (tax receipts) for reimbursement to generate cash for

the improper payments. Employees also allegedly engaged a travel vendor to submit fake or inflated invoices to generate cash to pay to the HCPs and created bank accounts in doctors' names.

The SEC also alleged that AZ China paid speaker fees to HCPs for speaking events that were completely fabricated. Even for events that were not fabricated, the SEC stated that the relevant speaking agreements lacked details such as the date of the event, venue, or subject matter.

Between 2006 and 2009, AZ China allegedly maintained written charts and schedules with the amount of forecasted or actual payments of maintenance fees, gifts, entertainment, and other expenses to individual doctors, departments, or hospitals. The SEC concluded that AZN's internal controls were deficient, and stressed that AZ China regularly reimbursed its employees for expenses that lacked adequate supporting documents and that certain members of the sales and marketing team circumvented formal approval procedures.

The SEC also alleged that from at least 2005 through 2010, AZ Russia (AstraZeneca UK Limited until 2007 and OOO AstraZeneca Pharmaceuticals from then onwards) provided corrupt incentives to government-employed HCPs. AZ Russia also purportedly maintained charts concerning HCPs, including their level of influence in purchasing decisions and means to court them.

According to the SEC, AZN violated the books and records provisions of the FCPA when its subsidiaries mischaracterized the improper payments to HCPs as legitimate expenses. AZN also failed to maintain sufficient internal controls relating to expense reimbursements, use of third-party vendors, speaker fees, and gifts, travel, entertainment expenses. In particular, while AZN had policies prohibiting the improper conduct of its subsidiaries, the SEC alleged that it failed to implement the policies effectively and monitor the activities of its subsidiaries in Russia and China. Among other things, AZN failed to conduct training for employees in high-risk positions in China and Russia and did not have in place adequate due diligence and monitoring mechanisms for third party business partners.

b. Cooperation and Remedial Measures

While noting that AZN did not self-report the violations, the SEC credited AZN for its "significant" cooperation including: (i) voluntarily disclosing information obtained during its own internal investigations, (ii) providing translations of key documents, and (iii) disclosing facts that the SEC would likely not have been able to discover by itself. The SEC also credited AZN for its remedial efforts to improve its compliance program before the SEC initiated its investigation. Finally, the SEC indicated that its decision not to impose a civil penalty in excess of \$375,000 was a result of AZN's cooperation.

5. Bahn, Ban, and Harris

On December 15, 2016, the DOJ filed a sealed indictment in the Southern District of New York against Ban Ki Sang ("Ban"), his son Joo Hyun Bahn ("Bahn"), and Malcolm Harris, for their involvement in a criminal scheme to bribe a foreign official. Ban and Bahn were both charged with one count of conspiracy to violate the FCPA's anti-bribery provision and three counts of violating the FCPA's anti-bribery provision. The DOJ also charged them each with one count of conspiracy to commit money laundering and one count of money laundering. Harris was charged with money laundering, wire fraud, and aggravated identity theft.

Ban, brother of former UN Secretary General Ban Ki Moon, was a senior executive at South Korean construction firm Keangnam Enterprises Co., Ltd (“Keangnam”). In early 2013, Keangnam was facing a cash flow crisis due to its maturing debts. Among other debts, Keangnam was facing maturity on loans it had taken to finance construction on a recently completed 72-story skyscraper complex in Hanoi, Vietnam (“Landmark 72”). The cost of the construction on Landmark 72 was approximately \$1 billion. Looking to secure an investor in Landmark 72 to ease its liquidity issues, Ban enlisted the help of his son, Bahn, a real estate broker at a Manhattan brokerage firm.

Bahn and Ban ultimately zeroed-in on a sovereign wealth fund from a Middle Eastern country as the target investor. Bahn initially tried and failed to use family influences to convince officials from the unnamed country to invest in Landmark 72. Ban was subsequently introduced to Harris, who presented himself as an agent for a high-ranking foreign official in the unnamed country with the ability to influence investment decisions of the sovereign wealth fund. Harris indicated that the foreign official would cause the sovereign wealth fund to purchase Landmark 72 for \$800 million in return for bribe payments. Ban and Bahn ultimately agreed to pay Harris \$500,000 up front and \$2 million upon the close of the sale of Landmark 72 with the expectation that Harris would pass these payments on as bribes to the foreign official.

In order to conceal the payments, Bahn caused Keangnam to enter into a formal agreement with Ban’s brokerage firm in which the brokerage firm was promised a percentage of the sale price of Landmark 72. In April 2014, Bahn and Ban caused Keangnam to transfer \$500,000 through two separate transactions to the brokerage firm’s account in New York as an “advance deposit” that was to be credited against the brokerage firm’s commission.

In order to pay Harris, Bahn obtained the assistance of a co-worker, San Woo, at his brokerage firm. Using the \$500,000 advance from Keangnam as collateral, Bahn and Woo were able to secure a loan from Woo’s business partner for \$500,000 paid directly to Muse Creative Consulting LLC, a company controlled by Harris. Woo’s business partner wrote a check to Muse Creative Consulting on the same day that Bahn’s brokerage received the \$500,000 advance from Keangnam.

Unbeknownst to Ban and Bahn, Harris had fabricated his relationship with the Middle Eastern foreign official. To this end, Harris forged emails to Ban and Bahn that were purportedly sent by the foreign official. When Ban and Bahn transferred the initial \$500,000 installment to Harris (to be passed along to the foreign official), Harris pocketed the payment himself. He spent the \$500,000 payment on lavish personal expenses, including the lease of a luxury penthouse condominium in Williamsburg, Brooklyn.

Harris was charged with one count of wire fraud, one count of aggravated identity theft, and one count of money laundering. On June 21, 2017, Harris pleaded guilty to wire fraud and money laundering. He also consented to forfeit \$500,000. On October 5, 2017, Harris was sentenced to 42 months in prison.

The case against Bahn is currently pending before Judge Edgardo Ramos of the S.D.N.Y. Ban is a fugitive presumed to be in hiding in South Korea. The DOJ also charged Woo, a resident of New Jersey, in a separate complaint with conspiring to violate the FCPA by helping Bahn funnel the \$500,000 bribe to Harris.

6. Embraer

On October 24, 2016, Embraer S.A. (“Embraer”), a Brazil-incorporated and São Paulo-based commercial jet manufacturer, agreed to pay a total of more than \$204 million to settle charges with the DOJ, SEC, and Brazilian authorities related to corrupt payments made by Embraer in connection with its activities in the Dominican Republic, Saudi Arabia, Mozambique, and India.

Throughout the relevant period, Embraer, the world’s largest manufacturer of mid-sized commercial jets and a leading Brazilian exporter, made its shares available in the United States through ADRs traded on the New York Stock Exchange and registered its common shares with the SEC pursuant to Section 12(b) of the Exchange Act. Furthermore, Embraer maintained its North American regional office in Fort Lauderdale, Florida and made several payments from the U.S. bank accounts of its wholly-owned Delaware-incorporated subsidiary Embraer Representations LLC (“Embraer RL”). As such, for all relevant periods, Embraer was a covered issuer within the meaning of the FCPA and subject to U.S. jurisdiction.

a. Dominican Republic

Starting in mid-2007, Embraer began to try to sell Super Tucano aircraft to the Dominican Fuerza Aérea de República Dominicana (“FAD”). By mid-2008, Embraer had successfully negotiated a deal that was pending only approval of the deal’s terms and financing by the Dominican Republic Senate. In order to help ensure Dominican Senate approval, an Embraer executive from its Defense and Government Market Division (“Executive A”) began discussing with Embraer’s primary contact at FAD a plan to influence the Dominican Senate. In early September 2008, Executive A agreed to pay the FAD official 3.7% of the sales value of the contract into three Dominican shell companies with the understanding that several “4 star” generals within the Dominican military would ultimately receive the funds and that the Dominican Senate would in return approve the transaction.

In December 24, 2008, the Dominican Senate approved the purchase of eight Super Tucano aircraft for approximately \$96.4 million. Embraer RL subsequently wired \$100,000 from its New York bank account to one of the Dominican shell companies agreed to by Executive A and the FAD official. In late September 2009, an executive from Embraer’s Legal Department advised that future payments to the FAD official should be made through a third-party agent (“Agent A”) rather than directly to the specified Dominican shell companies. In order to accomplish this, Embraer RL entered into a sham agency agreement with Agent A to pay Agent A an 8% commission on any successful sales of aircraft to the Jordanian Air Force. Embraer then made upfront payments of \$2.5 million and \$920,000 to Agent A from its New York bank accounts in return for “sales promotion services” provided under the agreement. However, Agent A never pursued any sales with the Jordanian Air Force. It merely transferred more than \$3 million to bank accounts as directed by the FAD official.

b. Saudi Arabia

In 2007, Embraer learned that a state-owned Saudi Arabian instrumentality planned to purchase executive jets to replace some of its aging fleet and had narrowed its choices to aircraft produced by Embraer and a competitor. Acting on this information, an executive from Embraer’s Executive Jets Division (“Executive B”) met in London with a senior official at the Saudi instrumentality with influence over the Saudi instrumentality’s purchasing decision. In exchange for a commission fee, the Saudi official

offered not only to assist Embraer win the contract but to convince the Saudi instrumentality to purchase new, rather than used, aircraft. Executive B agreed to pay the Saudi official \$550,000 per aircraft after receiving approval from his supervisor.

In order to conceal payments to the Saudi official and to circumvent certain internal controls, Embraer executives approved an agency agreement between Embraer RL and a South African sales agent (“Agent B”). Executive B had a preexisting personal relationship with Agent B. However, Agent B had no experience in the aviation industry or of doing business in Saudi Arabia. Agent B served only as a pass-through for the Saudi official and did not provide any legitimate services to Embraer. Despite there being no business justification to engage an unqualified, South African agent, Embraer executives were able to make payments to Agent B under the guise of an agency agreement to avoid internal controls which prevented (1) payments to entities in jurisdictions considered to be tax havens and (2) payments to employees of a customer.

On March 15, 2010, Embraer and the Saudi instrumentality signed the purchase agreement for three new Embraer jets for approximately \$93 million. Embraer RL subsequently paid more than \$1.6 million from its New York bank account to Agent B. Agent B then passed on \$1.4 million to the Saudi official through another intermediary.

c. Mozambique

In 2008, Embraer submitted a formal proposal to a state-owned commercial airline in Mozambique for the sale of two E190 aircraft. In mid-August 2008, a Mozambican consultant approached Embraer and informed Embraer that it should make a “gesture” to certain Mozambican government officials when it delivered the first aircraft. Embraer executives believed the Mozambican consultant to be well-connected with the relevant officials and agreed to offer a “gesture” of \$50,000-\$80,000 per aircraft. By the end of August, Embraer received a phone call from the Mozambican airline’s CEO indicating that \$800,000 would constitute an acceptable “gesture” and that competing bids would be given priority over Embraer’s bid if it did not pay.

Embraer and the Mozambican airline executed a purchase agreement on September 15, 2008. On April 22, 2009, Embraer RL executed a sham consulting agreement with a company established by the Mozambican consultant in the Democratic Republic of São Tomé and Príncipe. The consultant agreement engaged the Mozambican consultant for sales support services for the sale of E190 aircraft to the Mozambican airline and was signed by a senior executive from Embraer’s legal department and an executive vice president. Pursuant to this fake consulting agreement, Embraer RL paid \$800,000 from its U.S. bank account to a Portuguese bank account managed by the Mozambican consultant. Embraer RL recorded these payments as “Sales Commission” in its books despite its knowledge that they had no connection at all to legitimate services rendered and were instead bribe payments.

d. India

In India, from 2005 through at least July 3, 2008, Embraer paid an Indian national (“Indian Consultant”) \$5.76 million to assist Embraer win an approximately \$208 million contract to develop three specialized military aircraft for the Indian Air Force. Embraer entered into a consultant agreement with a U.K. incorporated company (“U.K. Entity”) with ties to the Indian Consultant in January 2005. Indian laws prohibit the use of consultants on military bids and Embraer believed its relationship with the U.K. Entity

to be illegal under Indian law. Embraer and the U.K. Entity therefore went to great lengths to keep the agreement secret. For example, the parties placed the only copy of the executed agreement inside of a safe deposit box in London, which required the simultaneous use of two keys, one by Embraer legal and one by the U.K. Entity.

By early February 2005, less than a month after engaging the U.K. Entity, Embraer signed a Memorandum of Understanding with India's Defence, Research and Development Organisation ("DRDO"). However, Embraer did not execute the purchase agreement until July 2008. While its agreement with the U.K. Entity had expired, Embraer nevertheless agreed to pay \$5.76 million to the U.K. Entity. Embraer executives disguised these payments through a falsified and un-related consulting agreement. In November 2009, Embraer's Swiss-subsiary Embraer AG signed a consulting agreement with a Singapore-based company to provide sales support services to an unrelated customer in Austria. In exchange for vaguely-described marketing services, Embraer AG, with funds from Embraer RL's New York bank account, paid \$5.76 million to the Singapore company's Swiss bank account. In turn, the Singapore company transferred \$5.76 in three equal payments to its Singapore accounts and then to the Indian Consultant. Ultimately, these costs were mischaracterized as a "selling expense" in Embraer's books and records.

e. Terms of Resolution

As part of its DPA, Embraer admitted to one count of conspiracy to violate the anti-bribery and books and records provisions of the FCPA and one count of violating the internal controls provisions of the FCPA. Embraer agreed to pay a criminal penalty of \$107,285,090. The criminal penalty represents a 20% discount from minimum penalty recommended by the United States Sentencing Guidelines. The DOJ considered several factors in deciding the applicable penalty, including Embraer's failure to self-disclose the violations, the seriousness and pervasiveness of the offenses throughout Embraer's three sales divisions, and the involvement of high level executives in each set of criminal conduct. The DOJ also considered Embraer's full cooperation with its investigation, Embraer's newly designed and implemented compliance program and internal controls, partial remediation and discipline of Embraer employees and executives who had been involved in the misconduct, and future continued cooperation with the DOJ.

The SEC alleged that Embraer violated the anti-bribery, books and records, and internal controls provisions of the FCPA. In connection with its settlement with the SEC, Embraer agreed to pay \$83.3 million in disgorgement and \$14.4 million in prejudgment interest. As part of its agreements with the DOJ and SEC, Embraer was also required to retain a corporate compliance monitor for a period of three years.

Internationally, Embraer also agreed to pay \$20 million in disgorgement to settle charges with Brazilian authorities. This amount will be credited against the amount paid to the SEC. In addition, Brazilian authorities charged eleven individuals in relation to Embraer's misconduct in the Dominican Republic and Saudi Arabian authorities charged two individuals in relation to Embraer's misconduct Saudi Arabia.

7. General Cable

On December 22, 2016, General Cable Corporation (“General Cable”), a Kentucky-based manufacturer and distributor of cable and wire, entered into a non-prosecution agreement with the DOJ to resolve allegations that General Cable’s foreign subsidiaries made corrupt payments to government officials to obtain and retain business in Angola, Bangladesh, China, Indonesia, and Thailand. On December 29, 2016 General Cable entered into a settlement with the SEC related to the same conduct. The SEC claimed that General Cable’s conduct amounted to violations of the anti-bribery, books-and-records, and internal controls provisions of the FCPA.

As part of its settlement with the SEC, General Cable agreed to pay disgorgement and prejudgment interest in the amount of approximately \$51 million. As part of its NPA, General Cable agreed to pay a monetary penalty of approximately \$20.5 million and disgorgement of approximately \$51 million (credited against the disgorgement paid to the SEC). Karl Zimmer, General Cable’s former Senior Vice President responsible for sales in Angola, agreed to pay a \$20,000 civil penalty to the SEC for causing General Cable’s violation of books and records and internal controls provisions of the FCPA by approving improper commission payments to an agent in Angola.

a. Corrupt Conduct

i. Angola

Between 2003 and 2013, two General Cable subsidiaries, Angola-based Condel and Portugal-based Celcat, made corrupt payments totaling \$9 million to employees of state-owned customers in Angola to increase sales to these customers. These payments were made both directly to employees at state-owned customers and through an agent (“the Agent”) with knowledge that the payments would be passed on to employees at the state-owned customers. These bribes allegedly resulted in more than \$34 million in profits. According to the SEC, with the use of the Agent, Celcat and Condel’s sales in Angola increased from \$6.7 million in 2009 to \$23.6 million in 2012.

For the first several years of the scheme, bribes were paid directly to five different employees at state-owned customers. These payments were orchestrated by the Country Manager at Condel but concealed from General Cable’s executive management. Beginning in 2009, Celcat and Condel concealed the payments through commissions paid to the Agent.

In 2012, General Cable executives, including Karl J. Zimmer, Senior Vice President of General Cable’s Europe and Mediterranean division (“EM”), received an internal audit report about General Cable’s subsidiaries in Angola that identified numerous red flags about the Agent. Among other things, the audit report noted that the agreement with the Agent did not contain anti-corruption language and that the commission rates were significant, ranging from 8% to 18.5 %. Despite these findings, payments continued until August 2013 when a Compliance Manager identified additional red flags, including payments to the Agent’s personal accounts. At this point, General Cable ceased payments to the Agent and launched a full internal investigation.

Because the decision to cease payments to the Agent pending the results of the internal investigation resulted in a loss or potential loss of approximately \$15 million in sales to Angolan state-

owned customers, Zimmer and other regional managers sought approval to continue using the Agent. General Cable's executive management instructed regional management to terminate the Agent's contract but allowed existing work with the Agent to continue on a case-by-case basis subject to "appropriate" and "proper" commission payments. A month later, Zimmer approved sales contracts with state-owned customers that called for commissions to the Agent from 7.5% to 18.5%. He also approved past due commissions to the Agent of 6% to 18% of the related sales contracts without supporting documents for the services provided.

ii. Bangladesh, Indonesia, Thailand

Between 2008 and 2013, General Cable's southeast Asian subsidiary, Phelps Dodge International Ltd ("PDTL"), made corrupt payments to state officials in Thailand, Indonesia, and Bangladesh.

In Thailand, between January 2008 and January 2013, PDTL paid more than \$5.4 million in payments to a Thai agent knowing that the agent would pass a portion of the payments to Thai state-owned customers. These corrupt payments allegedly resulted in profits of \$13 million. PDTL initially recorded the payments to the Thai agent as "success fees" but apparently, after realizing the term was indiscreet, later called them "rebates" or "cash discounts." Around 2012, a concerned PDTL executive told a General Cable regional executive about these potential bribes. Nevertheless, corrective action was not taken and the bribe payments did not stop until least a year later.

In Indonesia, from May 2011 to January 2014, PDTL made improper payments of more than \$2 million to two freight forwarders in connection with sales to an Indonesian state-owned customer that resulted in \$2 million in profits. PDTL failed to obtain proof of services provided by the freight forwarders, which allegedly had close ties to Indonesian government officials.

In Bangladesh, in September 2013, PDTL made an improper commission payment of \$43,700 to an agent when selling products to a Bangladeshi state-owned customer. The sales resulted in profits of \$85,759.

iii. China

Between December 2012 and 2015, General Cable (Tianjin) Alloy Products Company Limited ("GC China") made corrupt payments to Chinese agents and distributors totaling over \$500,000 on 19 projects with state-owned customers. Internal email communication at GC China revealed that GC China employees knew that a portion of these payments would be passed to employees of the state-owned customers. These corrupt payments were concealed in GC China's books as special discounts, technical service fees, design institute fees, and rebates.

iv. Egypt

According to the SEC, General Cable's subsidiary in Egypt provided or offered more than \$80,000 in bribes to employees of customers in suppliers in Egypt, some of which were state-owned entities. The SEC also alleged that General Cable provided small cash gifts or merchandise, such as laptops, and televisions, to employees of state-owned customers in Egypt as tips or holiday gifts.

b. Pilot Program

General Cable voluntarily self-disclosed its FCPA violations. Because the DOJ determined that General Cable also fully cooperated with the DOJ's investigation, took appropriate remedial action, agreed to enhance its compliance program and internal controls, and agreed to disgorge its illegally earned profits, General Cable met the requirements for the Pilot Program articulated in *Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance*. General Cable therefore received a 50% reduction off the bottom of the U.S. Sentencing Guidelines' penalty range, the highest reduction allowed under the Pilot Program in circumstances where the DOJ seeks a monetary penalty. General Cable also was not required to retain a corporate compliance monitor. General Cable must self-report to the DOJ and SEC on the status of the enhancements to its compliance program for a period of three years.

With respect to General Cable's cooperation, the DOJ noted that General Cable provided documents located abroad, flew foreign employees to the U.S. for interviews and made regular presentations to the DOJ on the status of General Cable's internal investigation. With respect to remedial measures, General Cable terminated or sought resignation from 13 employees who participated in the misconduct, three employees who failed to effectively supervise, and one employee who failed to take appropriate steps in response to the misconduct. General Cable also terminated 47 agents and distributors who participated in the misconduct.

8. GSK

On September 30, 2016, the SEC issued a cease-and-desist order against global pharmaceutical company GlaxoSmithKline plc ("GSK"). The SEC found that GSK violated the FCPA's books and records and internal controls provisions with respect to GSK's Chinese subsidiaries. Without admitting or denying the SEC's findings, GSK consented to the order and agreed to a \$20 million civil penalty.

The SEC and the DOJ began parallel investigations into GSK's Chinese business practices in 2010, as part of an industry-wide inquiry. According to a statement released by GSK, the DOJ concluded its investigation and informed GSK it will be taking no further action. The SEC settlement follows GSK's 2014 bribery conviction in a Chinese court and a fine in excess of \$490 million.

The SEC's findings relate to GSK's sales and marketing operations in China between at least 2010 and June 2013. GSK ran its Chinese distribution operations through its wholly-owned indirect subsidiary, GlaxoSmithKline (China) Investment Co Ltd ("GSKCI"), which was incorporated in the U.K. GSK also engaged the marketing and sales services of Sino-American Tianjin Smith Kline & French Laboratories Ltd ("TSKF"), a public-private joint venture in which GSK indirectly owns 55 percent.

a. Improper Payments

According to the SEC, employees and agents of GSKCI and TSKF engaged in a number of improper payment schemes directed at foreign officials, including healthcare professionals ("HCPs") and hospital administrative staff. These improper payments—including gifts, improper travel and entertainment, and even cash—served to generate increased prescription orders and purchases of GSK pharmaceutical products. For example, one sales representative submitted a work plan explaining that free boxes of prescribed product and holiday gifts would be exchanged for guarantees of monthly product orders.

The improper payments made by GSKCI and TSKF were falsely recorded as legitimate business expenses in GSK's books, including as medical association payments, travel and entertainment expenses, speaker fees, and marketing costs." Based on these findings, the SEC concluded that GSK violated the FCPA's recordkeeping provision. Additionally, the lack of adequate accounting controls coupled with GSK's failure to detect three years of improper payments led the SEC to find a violation of the FCPA's internal controls provision. While the SEC scrutinized GSK's behavior in general, it singled out and condemned specific schemes that GSKCI and TSKF had employed to cover improper payments.

The SEC alleged that GSKCI engaged third party vendors, whose inflated or entirely fraudulent invoices for travel and planning services served as a cover for payments to HCPs. From 2010 to June 2013, GSKCI spent RMB 1.4 billion (\$225 million) on travel and planning services. According to the SEC, these vendors were often engaged at inflated prices or for services that never occurred.

The SEC also alleged that GSKCI employed a speaker fee scheme to improperly influence HCPs. Although GSK placed hourly and yearly limitations on speaker fees for HCPs, GSK lacked any system that properly identified and tracked speakers engaged by its Chinese subsidiaries. As a result, RMB 14 million (\$2.2 million) out of GSKCI's total speaker fees expenditure of RMB 106 million (\$17 million) were allocated to HCPs whose identities could not be verified. The SEC concluded that these excess funds, which remain unaccounted for as legitimate speaker fees, were used as improper payments to HCPs.

Third, GSKCI used marketing programs as a pretext for improper payments and gifts to HCPs, according to the SEC. The SEC noted one marketing program in particular, the Cold Chain Project, which was originally designed to provide clinics with equipment to facilitate the storage and use of certain types of vaccines. However, instead of medical equipment, the program was used by GSKCI to provide HCPs with gifts such as laptops, tablets, and other electronic devices. In total, GSKCI spent approximately RMB 14.6 million (\$2.3 million) on gifts for clinics selected for their potential to market additional pharmaceutical products. The project was created and administered by senior marketing and sales managers of GSKCI.

b. Compliance Culture and Oversight

Aside from improper payments and weak accounting controls, the SEC also expressed concern about the corporate culture within GSK and its Chinese subsidiaries. The SEC emphasized that the improper practices described above were pervasive and were condoned by GSKCI and TSKF managers. The SEC also noted GSK's unresponsiveness in the wake of internal audits that revealed corporate culture issues. For example, a 2010 internal audit highlighted that unclear GSK policies coupled with high staff turnover led to confusion among commercial and medical staff regarding compliance policies and procedures. This confusion led to the approval of many non-compliant activities. Moreover, even when internal audits did correctly identify improper payments, they were dismissed as one-off incidents, as opposed to systemic controls deficiencies.

c. Remedial Action

In its order, the SEC recognized the remedial action taken by GSK, as well as GSK's cooperation with SEC staff during the investigation. In addition to prompt and continuous updates to the SEC regarding its own internal investigation of its Chinese and other operations, GSK also made significant

changes to the more problematic aspects of its business operations, including eliminating most payments to doctors and altering the compensation structure for sales representatives. GSK additionally bolstered its compliance program (including increasing third-party audits and employee anti-bribery training.

d. Settlement Terms

In addition to the \$20 million civil penalty and cease and desist requirements, the SEC ordered a two-year reporting program, whereby GSK will: (1) periodically update the SEC on its remediation and development of its compliance program; and (2) disclose any newly discovered evidence related to FCPA violations. Within this two-year period, GSK must conduct a set of reviews and submit certain reports regarding its findings to the SEC.

9. 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 Kinometrics, based in California. Over the course of the relevant period, Guralp paid approximately \$650,000 and Kinometrics paid approximately \$386,000 toward what Chi sometimes called his “advice fee.” Guralp and Kinometrics 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 Kinometrics overshadowed Chi’s legitimate salary “by a substantial margin.”

In exchange for Guralp’s and Kinometrics’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.

10. JP Morgan Securities

On November 17, 2016, JPMorgan Chase & Co. (“JPMorgan”) and its wholly-owned Hong Kong subsidiary, JPMorgan Securities (Asia Pacific) Limited (“JPMorgan APAC”), agreed to pay approximately \$264.4 million in penalties and disgorgement to settle claims with the DOJ, SEC, and Federal Reserve Bank of New York related to the hiring practices of JP Morgan APAC in China.

a. Sons and Daughters Program

From 2006 to 2013, JPMorgan APAC bankers created and managed a hiring scheme (dubbed the “Sons and Daughters Program” by JPMorgan APAC employees) for candidates referred by client executives or influential government officials in exchange for help securing business in China. Under the operation of the program, well-connected but often underqualified candidates bypassed JPMorgan’s standard hiring process and were awarded prestigious employment opportunities. Over a period of roughly seven years, JPMorgan APAC obtained a number of investment banking mandates from Chinese state-owned-enterprises (“SOEs”) through the program that generated over \$100 million in revenue for JPMorgan APAC and its affiliates. JPMorgan APAC alone profited more than \$35 million from the scheme.

At the inception of the Sons and Daughters Program, *quid pro quo* hiring only occurred in select instances. However, around November 2009, executives and senior bankers at JPMorgan APAC began to prioritize candidates connected to upcoming transactions, institutionalizing the “hiring for business” practice. Under the revised program, in order to be considered for employment, a candidate needed to be specifically linked to a business opportunity. To monitor and measure the revenue arising from these

hires, JPMorgan APAC maintained spreadsheets tracking the referred employees alongside revenues and specific clients.

JPMorgan APAC's internal communications revealed that many of the referral hires were unqualified for the job and performed low-level tasks not befitting the position. One hire was referred to as a "photocopier," another exhibited "undeniable underperformance," and a third was viewed as the worst business analyst candidate certain managing directors had ever seen. Regardless, the company bestowed the same titles upon referral hires—and paid them the same salaries—as entry-level investment bankers.

b. Anti-Corruption Policy and Internal Controls

JPMorgan and JPMorgan APAC were aware that the "hiring for business" practice potentially violated the FCPA. As early as 2001, JPMorgan's compliance policy noted the FCPA risks involved in hiring family members of foreign officials. In 2011, JPMorgan issued an updated anti-corruption policy, which provided that "[n]o employee may directly or indirectly offer, promise, grant or authorize the giving of money or anything else of value to a government official to influence official action or obtain an improper advantage." A training presentation made it clear that employment and even internships may constitute bribery under the policy.

In 2006, to enhance the screening process in light of the referral program's inherent FCPA risks, JPMorgan APAC's legal and compliance team designed a special questionnaire for potential referral hires. Each JPMorgan APAC banker requesting a new hire through the Sons and Daughters Program had to complete the questionnaire and seek approval from JPMorgan APAC's legal and compliance staff. Among other things, the questionnaire asked whether: (i) the applicant was qualified and had gone through the normal interviewing process; (ii) the referral was made by a person or entity related to the government; (iii) JPMorgan APAC was actively soliciting business from the referring individual or entity; and (iv) there was an "expected benefit to JPMorgan" should JPMorgan APAC hire the candidate.

The questionnaire failed to deter misconduct in the hiring process, and JPMorgan APAC even used the questionnaire to further conceal its corrupt business arrangements. JPMorgan APAC investment bankers omitted or outright falsified information in the questionnaires in order to receive compliance approval. Further, legal and compliance employees sometimes helped construct or alter responses to the questionnaire in order to conceal the true nature of the hire, allowing the candidate to withstand initial scrutiny. In approximately January 2007, JPMorgan APAC support personnel, including compliance staff, began using a questionnaire template with prepopulated answers that concealed the true purpose of the hire. For example, a question asking how the hire would benefit JPMorgan APAC was answered "[n]o expected benefit" by default. As a result, JPMorgan APAC's legal and compliance personnel did not reject a single candidate in the Sons and Daughters Program from 2007 through 2012, and the program continued to operate until a compliance officer in a new position rejected a referral hire in 2013.

c. Resolution of the Claims

JPMorgan agreed to pay the SEC \$130.5 million in disgorgement and prejudgment interest to settle charges that it violated the FCPA books and records, internal controls, and anti-bribery provisions through the Sons and Daughters Program. JPMorgan also agreed to pay a civil penalty of \$61.9 million in connection with a cease-and-desist order issued by the Federal Reserve Bank of New York for "unsafe

and unsound” hiring practices. JPMorgan APAC entered into a Non-Prosecution Agreement (“NPA”) with the DOJ that included a \$72 million penalty.

The DOJ fine against JPMorgan APAC represented a 25% discount off the bottom of the U.S. Sentencing Guidelines fine range. The DOJ indicated that the discount reflected JPMorgan’s and JPMorgan APAC’s cooperation with the investigation and the companies’ “extensive remedial measures.” These measures included terminating responsible individuals, levying over \$18 million in sanctions against current and former employees involved in the scheme, implementing elevated and centralized control measures over hiring programs, and increasing resources dedicated to compliance, especially in the Asia-Pacific region.

In addition to the fines and penalties, JPMorgan must implement a corporate compliance program and provide periodic self-reports to the DOJ and SEC on the status of the implementation of the compliance program for a period of three years.

11. Johnson Controls

On July 11, 2016, the SEC announced a settlement with Johnson Controls, Inc. (“JCI”), a NYSE-listed multinational with headquarters in Wisconsin. The SEC Cease-and-Desist Order alleged that JCI’s Chinese subsidiary, China Marine, made payments to sham vendors between 2007 and 2013 in violation of the FCPA’s books and records and internal controls provisions. JCI neither admitted nor denied the SEC’s findings. JCI agreed to pay to the SEC, \$14,362,561, consisting of \$11.8 million in disgorgement, a \$1.18 million in civil penalty, and \$1,382,561 in prejudgment interest. JCI also agreed to self-report to the SEC on the status of its FCPA and anti-corruption compliance measures for one year. On the same day, the DOJ issued a Declination Letter to JCI in connection with the same misconduct.

JCI, a multinational conglomerate, operates in 150 countries where it provides automatic temperature control systems for buildings, industrial facilities, and ships. China Marine is part of JCI’s global marine’s “Building Efficiency” business, and designs, sells and services marine refrigeration and HVAC systems in China through two legal entities, York Refrigeration Marine (China) Ltd (“YRMC”), and JCI Marine (Shanghai) Trading Company Ltd., both of which are described as wholly-owned indirect JCI subsidiaries.

a. Previous Misconduct by YRMC

JCI acquired YRMC as part of its 2005 acquisition of York International Corporation (“York”). In 2007, York, a Pennsylvania-based global provider of HVAC products and services, agreed to pay over \$12 million for FCPA violations, including misconduct arising out of the Iraqi Oil-for-Food scandal. The settlement with York also involved illicit payments by YRMC to agents and Chinese government officials between 2004 and 2006. As part of that settlement, York retained an independent compliance monitor that reviewed the effectiveness of controls within its operations and until 2010, reported its findings to JCI. Although JCI made enhancements to its compliance program, these were ultimately ineffective as they failed to detect and deter subsequent violations by certain subsidiaries, as is described below.

b. SEC Settlement

According to the SEC Order against JCI, from 2007 to 2013, China Marine's Managing Director and approximately 18 employees in three offices orchestrated an embezzlement and bribery scheme involving \$4.9 million in improper payments made to or through approximately 11 vendors to employees of state-owned shipyards, ship owners and others. The SEC determined that these payments resulted in \$11.8 million in benefits to JCI.

The scheme purportedly involved participation by, or knowledge of, a majority of China Marine managerial and other personnel. First, the Managing Director approved requests for adding vendors with undisclosed affiliations with China Marine sales managers. Upon approval, sales managers generated purchase orders for bogus costs for parts and services from these vendors and submitted the purchase orders to the Procurement Manager for approval. The fake purchase orders were then transferred to the Finance Manager, who authorized the payments, often without required supporting documentation. The proceeds from the transactions with these vendors was returned to employees' personal bank accounts, where it was used to make payments to employees of Chinese state-owned customers and for personal enrichment.

Through the above arrangement, China Marine employees effectively circumvented JCI's risk-based compliance procedures. The employees intentionally utilized a scheme involving vendors considered to be "low risk" due to the value of the transactions and lack of obvious contact with government officials. For instance, the average value of the transactions was \$3,400, an amount that avoided scrutiny and additional oversight from the JCI entity in Denmark responsible for overseeing China Marine's operations.

The SEC determined that throughout this six-year period, China Marine operated with limited oversight. Although JCI's Denmark office was responsible for supervising China Marine, the China Marine Managing Director largely had unfettered autonomy and JCI relied on his ability to supervise the operations. However, the Managing Director not only organized the illicit schemes but instructed employees to refrain from disclosing the payments to JCI lawyers, accountants, and auditors, and to avoid or delete related documentation.

The SEC concluded that JCI failed make and keep books, records, and accounts that fairly and accurately reflected its transactions. The agency also stressed JCI's failure to devise and maintain an internal accounting controls system that would have reasonably prevented and detected FCPA violations by China Marine, a high-risk subsidiary whose violations were considered to have been reasonably foreseeable based on historical failures. The SEC found that JCI's oversight was insufficient despite multiple compliance trainings provided to China Marine employees and periodic audits conducted on the company.

In particular, the SEC pointed to JCI's ineffective adoption of the independent monitor's recommendations to more closely integrate its marine business within the group's compliance culture, as well as JCI's decision to transfer oversight of China Marine to a newly hired, largely autonomous Managing Director. While China Marine was required to report to JCI's Denmark office, only a few transactions reached the reporting thresholds, and the SEC questioned whether managers in Denmark were sufficiently familiar with China Marine's operations to identify improprieties. The SEC Order also

found that JCI failed to ensure that its audit and testing procedures would adequately review payments that were routinely below the testing thresholds. The lack of controls resulted in JCI's failure to detect misconduct until the first of two anonymous whistleblower reports made in December 2012, after the Managing Director's resignation.

Nonetheless, JCI self-reported the potential violations to the SEC and the DOJ in June 2013, shortly after it retained outside counsel to conduct internal investigations, and approximately one month after it received a second anonymous whistleblower complaint. The SEC commended JCI's thorough, complete, and timely cooperation in reporting and subsequent investigations. JCI provided to the agency, factual chronologies, "hot" document binders, interview summaries, and translations of numerous emails and documents. In addition to making local and foreign employees available for interviews, JCI provided "real time" reports of employee interviews, and took steps to secure and preserve evidence when it caught a Chinese employee shredding documents.

The SEC further acknowledged JCI's remedial efforts including the termination of 16 employees implicated in the illegal schemes. JCI also placed all suspect vendors on "do-not-use/do-not-pay" lists, closed down China Marine's offices, and transferred all remaining employees (which did not include sales or procurement personnel) to other subsidiaries. JCI additionally enhanced its integrity testing and internal audits to include enhanced scrutiny of vendor on-boarding, and now implements random site audits to assure delivery of goods on purchase orders.

c. DOJ Declination

The DOJ's Declination Letter cited the FCPA Pilot Program as the basis for its no-action relief against JCI. According to the DOJ, the case against JCI was closed for the company's voluntary disclosure of misconduct, the thoroughness of its internal investigations, and full cooperation as reflected in its provision of all known relevant facts to the DOJ, along with its agreement to continue to cooperate with any ongoing investigations of individuals. The DOJ also highlighted JCI's disgorgement and civil penalty to the SEC, its enhanced compliance program and internal accounting controls, and full remediation, including termination of employees and high-level executives involved in the misconduct.

12. Key Energy

On August 11, 2016, Key Energy Services, Inc. ("Key Energy"), a Houston-based provider of onshore energy production services that is listed on the New York Stock Exchange, agreed to pay \$5 million in disgorgement to resolve internal controls and books and records violations in connection with the conduct of its Mexican subsidiary, Key Mexico. Key Mexico had made approximately \$561,000 in illegal payments via a consulting firm to an employee of Petróleos Mexicanos ("Pemex"), a Mexican state-owned company, between August 2010 and May 2014. The SEC Cease-and-Desist Order ("Order") noted that it did not impose a penalty in addition to the imposed disgorgement in part because of Key Energy's vulnerable financial condition, and the Order included a provision governing payment of disgorgement in the event the company goes into bankruptcy. In April 2016, Key Energy disclosed that the DOJ had declined to prosecute related misconduct.

Key Energy provides rig-based services to major oil and gas companies across the United States, Mexico, Colombia, Russia, and the Middle East. In September 2015, the company announced its failure

to meet the NYSE continued listing standard of \$1 minimum trading price. The company's shares continued to trade below this threshold, and on July 27, 2016, Key Energy announced that it would not contest the NYSE determination to commence de-listing of its stock. Moody's also downgraded the company's bonds to highly speculative, and Key Energy now trades on the over-the-counter markets.

The following summary is based on the facts alleged by the SEC in its administrative order; Key Energy was not required to admit or deny the SEC's factual allegations.

a. Payments to Pemex Employee through Sham Consultancy Company

Key Mexico hired the consulting firm in approximately August 2010. The SEC found no evidence that the consulting firm ever provided genuine services; instead, it appears to have been a vehicle for conveying payments to an official who worked in the Pemex department that negotiated and approved certain contracts. Of the \$561,000 paid to the Pemex employee through the consulting company, at least \$229,000 in payments were improperly described in Key Mexico's accounting system as "expert advice on contracts with the new regulations of Pemex/Preparation of technical and economic proposals/contract execution." In exchange for the payments, the Pemex employee assisted Key Mexico with bidding for contracts, lobbying for lucrative amendments to existing contracts, and by providing non-public information about tenders. The Pemex employee's connection to the consultancy company was known to Key Mexico's Country Manager, who also paid approximately \$6,400 from his personal account to the Pemex employee's personal account.

We note that Key Energy is not the first company to come under scrutiny for alleged bribes paid to Pemex officials. The FCPA settlements involving Hewlett-Packard (2014), Bridgestone (2011), and Paradigm (2007) each involved underlying conduct including bribery of Pemex officials.

In 2011, Key Energy became aware of the relationship between its Mexican subsidiary and the consulting firm, although Key Energy did not learn of the connection to the Pemex employee. Nonetheless, Key Energy allowed the relationship to continue despite several violations of its own internal compliance program, including (i) the relationship had not been pre-approved by the parent company; (ii) there was no written contract between the subsidiary and the consultant; and (iii) no due diligence had been performed on the consultant. Key Mexico also allowed payments to be made to the consultant despite not having adequate proof of services documentation. Key Mexico finally regularized its relationship with the consultant through a written contract two years later, in 2013. Key Energy and Key Mexico never conducted due diligence, and therefore Key Energy did not discover the relationship between the Pemex official and the consultancy company until 2014, when the SEC notified Key Energy of its concerns and Key Energy launched its own internal investigation.

b. Christmas Raffle Gifts to Pemex Officials

The SEC also highlighted Key Energy's failure to examine \$118,000 in gifts provided by Key Mexico to Pemex officials, and approved by Key Energy on the understanding that the gifts were for a Pemex company Christmas party raffle. First, Key Mexico hid from its parent company the fact that \$55,000 of the gifts were not actually earmarked for the raffle, but were instead given to "approximately 130 specific Pemex officials working in the regions in which Key Mexico operated." Second, the SEC noted that Key Energy failed to consider that the \$118,000 donation was 26 times larger than the raffle donation Key Mexico made the prior year. The Order stated that Key Energy "failed to respond effectively

to signs indicating that the gifts provided . . . were being given as rewards for providing Key Mexico with increased business that year” in part because Key Energy “failed to consider the implications of the explanation by Key Mexico’s country manager that the higher gift amount in 2012 was correlated to Key Mexico having done more business with Pemex that year.” The SEC noted that, if the parent company had asked for more information, it would have learned that its subsidiary was giving Christmas gifts to Pemex officials at the same time that the subsidiary was “engaged in ongoing negotiations with Pemex, including negotiations to obtain additional funding for work required under its contracts with Pemex.”

c. Cooperation and Remedial Measures

In January 2014, the SEC informed Key Energy that it was investigating potential FCPA violations. Key Energy commenced a broad internal investigation in response. The Mexico Country Manager resigned in February 2014. In April 2014, Key Energy reported its initial findings to the SEC, including information that the departed Country Manager had promised bribes to Pemex employees.

Crediting the company’s cooperation and “significant remedial measures” in the settlement, the SEC highlighted: (i) the appointment of a new Chief Compliance Officer who supervised the overhaul of Key Energy’s compliance program, and who visited each international location to conduct training for all international employees; (ii) the development of compliance policies and adoption of enhanced due diligence procedures for vendors; (iii) the suspension of payments to vendors and third parties in Mexico; (iv) the manual review of over 600 vendors, including targeted reviews of vendors in Russia and Colombia; (v) enhanced financial controls in Mexico, Colombia, and Russia; (vi) an enhanced corruption risk assessment process; (vii) the hiring of new controllers in Colombia and Mexico, and enforcing reporting to the U.S. Controller and the CFO; and (viii) the coordinated exit of all markets outside North America, including Mexico.

13. LATAM Airlines, LAN Airlines, and Ignacio Cueto Plaza

On July 25, 2016, LATAM Airlines Group S.A. (“LATAM”), as successor-in-interest to LAN Airlines S.A. (“LAN”), agreed to pay \$22 million to the DOJ and SEC to resolve criminal and civil FCPA books and records and internal controls violations for misconduct in Argentina. LATAM admitted that executives of LAN and of its subsidiaries paid bribes to Argentine labor union officials through a fictitious \$1.15 million contract with a third party consultant. In return, the unions agreed to refrain from enforcing certain contractual terms and labor rules, which resulted in an estimated benefit of \$ 6,743,932 in decreased labor expenses to LAN’s Argentine subsidiary. In February 2016, the SEC settled related books and records and internal controls charges with LAN CEO, Ignacio Cueto Plaza, who paid a \$75,000 civil penalty and committed to a number of compliance obligations.

LATAM is a NYSE-listed airline holding company based in Chile, with operations across the Americas, Australia, and Europe. LATAM was formed as a result of a 2012 merger between Chilean airline LAN, and TAM Airlines S.A., a Brazilian company. Prior to the merger, LAN shares traded as ADRs on the NYSE, and the shares of LATAM continued to be traded as ADRs following the merger. All LAN subsidiaries, including Miami-based LAN Cargo and Atlantic Aviation Investments LLC (“AAI”), incorporated in Delaware, were subsequently merged into LATAM.

a. Union Negotiations, the One Function Rule, and a Consultant

In April 2005, LAN purchased 49% of AERO 2000, a non-operating airline in Argentina. The agreement required that LAN employ personnel of two other defunct airlines under pre-existing collective bargaining agreements ('CBAs'). Upon commencing operations, AERO 2000, renamed LAN Argentina S.A. ("LAN Argentina"), began experiencing increased demands from five labor unions that represented the workers it had acquired under the April 2005 arrangement. The unions threatened to enforce the "one function rule," provided in the CBAs, that restricted workers to a narrowly defined single role, and would have required LAN Argentina to double its workforce. Though rarely enforced in practice, the rule provided the unions with leverage, which was used during a contentious campaign for wage increases that also included strikes and work stoppages.

During the course of the campaign for wage increases, LAN Cargo's Vice President of Business Development was contacted by an Argentine lawyer (the "consultant") who, during the relevant period, served as a Cabinet Advisor to the Secretary of Argentina's Ministry of Transportation. The consultant offered to negotiate with the labor unions on LAN's behalf in return for a \$1.15 million payment that would be shared with parties who had influence over the unions. With approval of Mr. Cueto Plaza, the LAN Cargo VP agreed to engage the government official as a consultant.

The consultant successfully negotiated with the labor unions on LAN's behalf, resulting in an agreement to refrain from enforcing the one function rule against LAN Argentina for a four-year period and to a lower wage increase than initially sought, resulting in an overall benefit of approximately \$6.744 million to LAN. In October 2006, to support the \$1.15 million payment, LAN officials agreed to enter into a contract with the consultant for a fictitious study of Argentine and regional air routes and a legal analysis on Argentine law. Although neither the draft agreement nor the services were ultimately executed, the consultant's company submitted invoices to LAN, which made the payments to personal accounts owned or controlled by the consultant and his family members. The LAN Cargo VP directed the consultant to address three of four invoices to AAI, another LAN subsidiary, and the payments were recorded in AAI's books as made to "other debtors," and approved by LAN executives, including Cueto Plaza. Payments in excess of \$1 million were made to the consultant's brokerage account in Virginia, USA, while other payments were made to an account in Spain.

b. Terms of the LATAM DPA and SEC Order

The three-year DPA includes an independent compliance monitor for a period of not less than 27 months and a criminal penalty of \$12.75 million, a sum computed under the U.S. Sentencing Guidelines with a base fine of \$8.5 million and a 1.5 multiplier. The DOJ described several reasons why LATAM paid a criminal penalty within the U.S. Sentencing Guidelines range, rather than one discounted from the bottom of the sentencing range. For example, although LATAM ultimately fully cooperated, the DOJ described it as having failed to voluntarily disclose the misconduct in a timely manner, given that disclosure occurred only after press reports of investigations by Argentine and Chilean law enforcement, causing a four-year delay and the loss and destruction of potentially relevant evidence including through routine data retention policies. Further, while the company agreed to future cooperation with the DOJ, the DPA noted that LATAM failed to adequately remediate the misconduct and failed to discipline any of the responsible employees (including a high-level executive), which it described as undermining the effectiveness of its compliance program. The DOJ also identified the company's prior enforcement

history, including LAN Cargo's 2009 guilty plea for criminal conspiracy to fix prices in the airline cargo industry between 2003 and 2006.

In addition to improving its compliance policies and procedures, LATAM agreed to provide full disclosure and cooperation with any FCPA investigations of the company, its officers, directors, employees, agents, partners and consultants, and with regulatory and other enforcement agencies when requested by the DOJ. In connection with the DPA, the DOJ also agreed to conditionally release LATAM from civil and criminal liability for certain conduct concerning gifts, entertainment, and travel expenses to government officials in Argentina between 2005 and 2011, that had been disclosed to the DOJ prior to DPA.

In its settlement with the SEC, LATAM agreed to cooperate with other judicial or administrative proceedings, to appoint an independent compliance monitor, and to pay \$9,437,788, consisting of disgorgement and prejudgment interest. The SEC Order considered remedial steps taken by LAN and its successor entity, emphasizing the evolution of the company's compliance program from the initiation of a basic compliance program in 2008 and the engagement of a new General Counsel and Vice President of compliance to the 2013 adoption of a new Code of Conduct and other internal policies including on anti-corruption, gifts, travel, hospitality and entertainment, procurement and payments. The SEC noted that LATAM hired several compliance personnel, including a Compliance Manager who oversees a team of twenty.

c. LAN CEO Ignacio Cueto Plaza's \$75,000 Penalty and Remedial Actions

On February 4, 2016, the SEC announced that it had issued a Cease-and-Desist Order against Ignacio Cueto Plaza, the sitting CEO of LAN, in connection with his role in the conduct described above. Cueto was charged with causing LAN to violate the books and records and internal control provisions of the FCPA as a result of his role as President and Chief Operating Officer of LAN from 2005 until the airline merged with TAM in 2012, at which time he became the CEO of LATAM.

In settling the administrative proceeding, Cueto agreed, without admitting or denying the SEC's findings, to undertake a series of remedial actions and to pay a civil money penalty of \$75,000. The remedial actions included agreeing to complete any required anti-corruption and related ethics training required by LAN, which the SEC noted at a minimum would include annual live and online anti-corruption training, and cooperating with the SEC in connection with any related judicial or administrative proceeding or investigation. The SEC also noted that Cueto is now subject to LATAM's enhanced compliance structure and internal accounting controls and is required to certify compliance with LATAM's new Code of Conduct (adopted in 2013), as well as other internal corporate policies, including an Anti-Corruption Guide and a Gifts, Travel, Hospitality and Entertainment Policy. Cueto was credited with having attended Corporate Governance Training and provided a certification confirming acknowledgement of the Code of Conduct, and relevant applicable regulations and Company policies. Cueto also executed an amendment to his employment agreement under which he acknowledged being informed about LATAM's Manual for the Prevention of Corruption and that he is responsible for performing his duties in compliance with the highest ethical standards and all Company policies and procedures.

14. Las Vegas Sands

On April 7, 2016, the SEC imposed a settled cease-and-desist order against Las Vegas Sands Corp. (“Vegas Sands”) to resolve allegations that the Company had violated the books and records and internal controls provisions of the FCPA in connection with its operations in China and Macau. Under the settlement, Vegas Sands agreed to pay a \$9 million civil penalty to the SEC and retain an independent compliance monitor for a period of two years. On January 17, 2017, Vegas Sands entered into a non-prosecution agreement with the DOJ centering on the same conduct. Vegas Sands agreed to pay a criminal penalty of \$6.96 million. Vegas Sands also agreed to share with the DOJ the reports prepared by the corporate compliance monitor appointed as part of its settlement with the SEC.

Vegas Sands is a Nevada-based casino and resort operator that was founded by billionaire Sheldon Adelson. The Company owns and operates resorts and casinos in the U.S. and Asia through a network of subsidiaries and is traded on the NYSE.

According to Company filings, the SEC first subpoenaed Vegas Sands in February 2011 and requested that the Company produce documents relating to its FCPA compliance. At the same time, the Company also learned that the DOJ was conducting a similar investigation. Vegas Sands believed that the investigations were triggered by a 2010 lawsuit filed by Steven Jacobs, the former CEO of Sands China Ltd. (“Sands China”), a Vegas Sands subsidiary that is traded on the Hong Kong Stock Exchange. Jacobs’ lawsuit alleged breach of contract against Vegas Sands and Sands China, breach of the implied covenant of good faith and fair dealing, and tortious discharge in violation of public policy against Vegas Sands. His case devolved into a nearly six-year long discovery dispute before being resolved on May 31, 2016 through a confidential settlement.

The SEC alleged that between 2006 and 2011, Vegas Sands failed to devise and maintain a reasonable system of internal accounting controls over its operations in China and Macau and failed to accurately record various transactions in its books and records. The NPA and cease-and-desist letter focused on Vegas Sands’ relationship with a consultant in China who received over \$60 million during this time period.

In the fall of 2006, the then-Vice President of Vegas Sands Asian Development identified a former Chinese government official to serve as a consultant and assist the Company with its activities in China. Vegas Sands used the consultant’s services on a number of projects that involved significant internal controls failures, the most notable of these being Vegas Sands’ involvement with a Chinese basketball team, purchase of an office building in Beijing, and retention of a ferry management company.

a. The Basketball Team

In early 2007, Vegas Sands sought to purchase a professional basketball team in China in order to promote Vegas Sands and bring customers to the Vegas Sands-owned Venetian Macau, which has its own sports arena. Because a gaming company is not permitted to own a basketball team under the Chinese Basketball Association’s rules, Vegas Sands used a consultant as a front to buy the team. The consultant established an entity called Shenzen Wei Li Xin to purchase and own the team. One of Vegas Sands’ Chinese subsidiaries transferred over \$6 million to Shenzen Wei Li Xin in violation of Vegas Sands internal policies and procedures.

In September 2007, a Vegas Sands finance director raised concerns regarding the basketball transaction to the CFO of Vegas Sands. The finance director was particularly concerned with the repeated transfer of funds to the consultant without any supporting documentation regarding the basketball team's need for the funds or the manner in which they were used. The CFO instructed the director to conduct financial due diligence on the team that Vegas Sands was apparently sponsoring. However, the due diligence was obstructed by the consultant, who claimed that he could not contact their accountants to provide the requested information. Instead, the consultant allegedly had one of his employees prepare a handwritten list of the team's expenses. The SEC alleged that when the finance director continued to raise concerns about the team and the consultant, the President of Vegas Sands subsequently arranged to have the finance director placed on administrative leave and eventually terminated.

In October 2007, the CFO of Vegas Sands expressed a number of concerns internally regarding the basketball team, including the inability of Vegas Sands to track funds that it had transferred to the consultant and a lack of recourse if the consultant failed to purchase the team. In late 2007, Vegas Sands retained an international accounting firm to review the transaction. The consultant and the then-Vice President of Vegas Sands Asian Development significantly obstructed the accounting firm's process. For instance, they failed to grant the accounting firm access to key accounts that would have allowed the firm to complete its investigation. When the firm was instructed to cease its investigation in February 2008, it apparently had already identified over \$700,000 in unaccounted funds that had been transferred to the consultant.

According to the SEC, in total between March 2007 and January 2009, Vegas Sands paid approximately \$14.8 million to the consultant in connection with the basketball team pursuant to a series of sponsorship and advertising contracts. Approximately \$6.9 million of this amount was allegedly transferred without the appropriate authorizations or necessary supporting documentation.

b. Development of a Resort on Hengqin Island and the Beijing Business Center

According to the SEC, beginning in 2006, Vegas Sands' President sought to develop a resort on the Hengqin Island, a new resort district in China. The Vegas Sands President allegedly understood that any such development would need the approval of various governmental entities and sought to partner with a Chinese company that could improve Vegas Sands' ability to obtain the needed approvals. Vegas Sands' consultant allegedly introduced the Company to the chairman of a state-owned entity ("SOE") who was thought to have particular influence in connection with Hengqin Island.

According to the SEC, Vegas Sands initially attempted to form a joint venture with this state-owned entity. Under the proposed joint venture arrangement, Vegas Sands would make a real-estate investment by purchasing a building in Beijing from the entity and the entity would help Vegas Sands develop Hengqin. The SEC alleged that the chairman of the SOE and Vegas Sands' consultant indicated, however, that it would be necessary to have a third company involved in the relationship to act as a "beard" because the SOE's board would not approve a direct relationship with a casino operator.

Accordingly, instead of the joint venture, Vegas Sands' President approved using the consultant to purchase the Beijing building from the SOE. Vegas Sands apparently planned to turn the building into a

business center to assist U.S. companies seeking to do business in China. The building was to be named the "Adelson Center" and was scheduled to open in August 2008.

The SEC alleged that no research or analysis was done to determine whether the need existed for the business center or whether it was likely to generate a profit or loss. Numerous employees were apparently also concerned that the purchase was solely for political purposes. Nevertheless, between July 2007 and February 2008, approximately \$43 million was transferred to one of the consultant's entities to purchase the real estate.

Around mid-2007, the consultant demanded that Vegas Sands make an up-front payment of at least \$1.4 million so that the consultant could secure Vegas Sands' title to the unfinished basement of the building. Despite concerns from Vegas Sands employees and outside counsel that the payment could raise FCPA issues, in April 2008 a Vegas Sands subsidiary wired the consultant \$3.6 million as a pre-payment for a five-year lease on the basement. The consultant never provided any documentation or other evidence demonstrating that the consultant had ever purchased the basement from the SOE.

The DOJ identified a number of other payments made by Vegas Sands' subsidiaries to the consultant that illustrated a lack of effective internal controls and were misrepresented in Vegas Sands' books, including approximately \$1.4 million for "arts and crafts" procurement in April 2008, \$1.4 million for advertising in September 2008, \$1.4 million for marketing and promotional services in October 2008, and \$900,000 in property management fees between November 2008 and July 2009.

According to the SEC, Vegas Sands transferred approximately \$61 million to the consultant in connection with the real estate deal. After the project was cancelled in late 2008, Vegas Sands received only \$44 million of that sum back from the consultant.

c. Macau Ferry Operation

According to the SEC, in 2007 Vegas Sands set up a high-speed ferry business to transport customers from China and Hong Kong to Macau. Vegas Sands sought to contract with a ferry services provider to operate the ferries. Apparently under pressure from Vegas Sands President, Vegas Sands employees selected two entities: (1) a recently formed ferry company that was partially owned by a Chinese state-owned ferry company, and (2) a shipping company owned indirectly by Vegas Sands' consultant and the SOE Chairman. The SEC noted that Vegas Sands' President stated in an email that the selection of the newly formed ferry company would be politically advantageous. The SEC also indicated that the ferry company had an annual budget that included business entertainment. Even though Sands China's internal audit department found that the company was spending the majority of its entertainment expense on government officials, and had indicated that this expense was necessary to secure routes for ferries, the auditors failed to elevate this issue within the Company.

d. Additional Conduct

The SEC also alleged that Vegas Sands' internal accounting controls were deficient in a number of other areas. The Agency noted that even though Vegas Sands had a policy requiring backup documentation for reimbursement of payments to outside counsel in excess of \$100, this policy was not uniformly enforced and in 2009, an attorney was reimbursed for "expenses in Beijing" in the amount of \$25,000 without providing documentation to support the charges. According to the SEC, the attorney later

stated that he actually requested the funds on behalf of a friend who was an unpaid consultant to Vegas Sands. This payment was also allegedly recorded in the Company's books and records as a reimbursement of legal expenses, despite the lack of documentation.

The SEC also noted that Vegas Sands provided complimentary items and services, such as restaurant meals and hotel stays, to actual and potential gaming customers and business contacts in Macau. According to the SEC, however, casino employees often failed to record the recipients of these complimentary items, resulting in an inability to track or audit this practice or identify whether complimentary items were provided to government officials or politically exposed persons.

e. Cooperation and Remedial Efforts

In determining an appropriate resolution for this matter, the SEC indicated that it took into consideration Vegas Sands' cooperation with Commission staff and prompt remedial actions. Vegas Sands' Audit Committee retained outside counsel to conduct an internal investigation and shared the findings of the investigation with the SEC, providing information that otherwise may not have been available to SEC staff. Vegas Sands facilitated interviews with key foreign witnesses and voluntarily produced translations of key documents including large volumes of business, financial, and accounting records. Vegas Sands also hired a new general counsel and new heads of internal audit and compliance, and established a new Board of Directors Compliance Committee. In addition, Vegas Sands increased the compliance and accounting budgets, updated certain key documents including its Anti-Corruption Policy, and developed and implemented enhanced anti-corruption training and an electronic procurement and contract management system.

Similarly, the DOJ awarded Vegas Sands full credit for cooperation with its investigation and remedial actions. As a result, the criminal penalty assessed by the DOJ represents a 25% reduction off of the bottom of the Sentencing Guidelines fine range, the maximum allowed under current DOJ policy for a company that did not voluntarily disclose the violations.

15. Mexico Aviation Cases

Between December 2015 and March 2016, six individuals pleaded guilty to various charges related to the bribery of Mexican officials and private persons to secure aircraft maintenance and repair contracts in the U.S. and Mexico.

In October 2016, Douglas Ray, the president and owner of Global Aviation Services, and Victor Hugo Valdez, Global Aviation's sales agent in Mexico, each pleaded guilty to conspiracy to violate the FCPA and conspiracy to commit wire fraud. Between 2006 and 2016, Ray, including with the assistance of Valdez, paid bribes to at least seven Mexican officials to help Global Aviation Services win aircraft maintenance contracts. Four of these officials worked for Mexican states, including Tamaulipas, which borders southern Texas. The other three officials were responsible for overseeing the maintenance of a Mexican law enforcement agency's aircraft. Ray and Valdez made payments both in the U.S. and in Mexico, and concealed the bribes by inflating the aircraft maintenance contracts and passing the extra amounts on to the officials. The wire fraud conspiracy charges relate to Ray's and Valdez's scheme to bribe employees of private companies in the U.S. and Mexico to win additional aircraft maintenance contracts. After pleading guilty and cooperating with authorities, including by wearing a listening device,

Ray was sentenced to 18 months in prison and required to pay restitution of \$590,000, and forfeit \$2 million. Valdez was sentenced to 12 months in prison, paid restitution of \$90,000, and forfeited an additional \$275,000.

In November 2016, Kamta Ramnarine, a former owner and General Manager of Hunt Pam Am Aviation Inc., and Daniel Perez, also a former owner of Hunt Pan Am and the company's Director of Maintenance, pleaded guilty to conspiracy to violate the FCPA. Between 2007 and 2015, Ramnarine and Perez made improper payments to Tamaulipas officials to win aircraft maintenance contracts. Like Ray and Valdez, Ramnarine and Perez disguised the payments by inflating invoices and using the excess to pay the officials. Ramnarine and Perez were each sentenced to three years of probation.

In December 2015, Ernesto Hernandez Montemayor, the former director of aviation for the state of Tamaulipas, pleaded guilty to conspiracy to commit money laundering. Montemayor was sentenced to 24 months in prison and ordered to forfeit \$2 million. According to charging documents, Montemayor was one of the officials who received improper payments from Ray, Ramnarine, and Perez. In March 2016, Ramiro Ascencio Nevarez, a former pilot for the Autonomous University of Tamaulipas who received improper payments from Ramnarine and Perez, also pleaded guilty to money laundering and was sentenced to 15 months in prison. While Montemayor and Nevarez were both foreign officials at the time of the misconduct and therefore not subject to the FCPA, both were charged with conspiring to violate the federal money laundering statute that prohibits engaging in monetary transactions through financial institutions in property valued at greater than \$10,000 and derived from certain predicate statutes, which include the FCPA.

16. Nordion and Mikhail Gourevitch

On March 3, 2016, Nordion (Canada) Inc. ("Nordion Canada"), a privately held Canadian company that is a successor in interest to global health science company, Nordion, Inc. ("Nordion"), agreed to pay a civil penalty of \$375,000 to the SEC to settle allegations that Nordion violated the books-and-records and internal accounting controls provisions of the FCPA with respect to its application for governmental approval to distribute its liver cancer treatment, TheraSphere, in Russia. Prior to becoming a privately held company (and during the period relevant to the conduct described below), Nordion had its common stock registered with the SEC pursuant to Section 12(b) and was traded on the NYSE.

Separately, Mikhail Gourevitch, an engineer formerly employed by Nordion, agreed to pay \$178,950 to the SEC to settle allegations that he violated the anti-bribery, books-and-records, and internal controls provisions of the FCPA in connection with his role in the scheme. The SEC's settlement with Mr. Gourevitch, a dual Israeli and Canadian citizen, included disgorgement of \$100,000, prejudgment interest of \$12,950, and a civil penalty of \$66,000.

The settlements focus on Nordion's use of an agent between 2004 and 2011 to attempt to obtain approval to distribute TheraSphere in Russia. According to the SEC, during this period Nordion (i) failed to conduct virtually any due diligence on the agent; (ii) failed to provide adequate anti-corruption training to its employees; (iii) paid invoices even though they lacked detail and directed Nordion to make payments to offshore bank accounts for entities that were unknown to Nordion; and (iv) did not have adequate policies and procedures in place to detect corruption risks.

Although Nordion had reported the fact and results of its internal investigation to both U.S. and Canadian authorities, it was reported in March 2016 (following the SEC settlement) that the Royal Canadian Mounted Police closed their own investigation into this matter without taking further action against Nordion or Nordion Canada.

a. Use of Third-Party Agent in Russia

According to the SEC, during the summer of 2000, Mr. Gourevitch informed Nordion that his childhood friend in Russia could help the company purchase a medical isotope known as cobalt-60 from the Russian Government. Nordion had previously purchased cobalt-60 from the Canadian government and then resold the product to health care institutions. Soon thereafter, the company informally authorized the agent to meet with Russian officials on Nordion's behalf. Nordion subsequently signed a written consulting agreement with the agent in approximately March 2002, despite having performed little or no due diligence. The SEC noted that despite having no experience in the nuclear power industry, with nuclear medicine or with medical isotopes, the agent was successful in helping Nordion obtain the cobalt-60 supply contracts.

Following this success, Nordion enlisted the agent in 2004 to assist the company in obtaining approval from the Russian Government to distribute its liver cancer treatment, TheraSphere. Nordion entered into a contract with the agent to register, license and distribute TheraSphere and ultimately paid the agent a total of \$235,043 for this purpose between 2005 and 2011. Ultimately, however, the project was unsuccessful and Nordion was never able to distribute TheraSphere in Russia.

According to the SEC, Mr. Gourevitch, who remained Nordion's primary contact with the agent, knew that the agent intended to use a portion of its compensation from Nordion to bribe Russian officials in an attempt to obtain approval for the drug. The agent also allegedly returned at least \$100,000 of its fee directly to Mr. Gourevitch to compensate him for his role in the scheme.

The SEC alleged that Mr. Gourevitch and the agent explicitly discussed the scheme in email exchanges, which were conducted in Russian, apparently to avoid disclosure of the scheme. In one exchange cited by the SEC, Mr. Gourevitch is alleged to have altered cost estimates provided by the agent, which had included bribes to Russian officials as "unofficial costs" to "ensure the favorable acceptance of TheraSphere." Mr. Gourevitch is then alleged to have informed the agent (in Russian) that "Nordion does not want to see the bribes in your cost estimate and justification."

b. Disclosure and Cooperation

In August 2012, Nordion disclosed to the SEC and DOJ, as well as to Canadian authorities, that it had discovered evidence that improper payments may have been made to a Russian government official, and was conducting an internal investigation related to such payments. The SEC noted that it was refraining from imposing a greater penalty on the company in light of its cooperation with the investigation and remedial efforts, which included the fact that Nordion cooperated with investigations in both countries (including by making individuals available for interview) and hired outside counsel to revise its anti-corruption policies and procedures. The company's remedial measures included additional compliance staffing (led by a new Director for Corporate Compliance), as well as the incorporation of a compliance component as part of its annual employee performance reviews. Nordion also conducted additional anti-corruption, internal accounting controls and finance trainings to board members, management and

employees, and enacted an enhanced protocol for the use of third party agents, which requires all agents to enter into contracts that include FCPA warranties and representations and to adopt Nordion's anti-corruption policies.

17. Nortek

On June 3, 2016, the DOJ issued a declination letter to Nortek, Inc. ("Nortek"), a Rhode Island-based company listed on the NASDAQ Global Select Market. On June 7, Nortek also entered into a Non-Prosecution Agreement ("NPA") with the SEC, agreeing to pay \$322,058 (\$291,403 in disgorgement and \$30,655 in prejudgment interest) to resolve allegations that Nortek, through the actions of a Chinese subsidiary, violated the FCPA's internal controls and books and records provisions. In addition to the disgorgement and interest, Nortek reported that it spent over \$3.1 million in connection with its investigation by the end of fiscal year 2015.

Nortek manufactures and sells a range of construction, remodeling, computer, heating, and security products, and indirectly owns Linear Electronics (Shenzhen) Co. Ltd. ("Linear China"), a Chinese subsidiary at the center of the alleged misconduct. According to the NPA's Statement of Facts—which, in the event that Nortek breaches the NPA, Nortek agreed not to "dispute, contest, or contradict"—between 2009 and 2014, Linear China employees, including its managing director, accounting manager, and customs liaison officer made or approved improper payments including transfers of cash, gift cards, meals, travel, entertainment and accommodation to local Chinese officials "to procure preferential treatment, relaxed regulatory oversight, and/or reduced customs duties, taxes, and fees."

These improper payments were made at least monthly, over the five-year period, during which Linear China made over 400 transactions totaling approximately \$290,000 to officials in China's customs, environmental protection, health inspection, labor, police, telecommunications, and tax agencies. Based on the total amount and number of reported transactions to numerous recipients (approximately \$290,000 paid in over 400 transactions), the average size of each improper payment was under \$750.

The SEC found that Nortek's failure to devise and maintain a system of internal controls enabled the scheme to go undetected during the period, and that Nortek failed to notice obvious red flags in Linear China's financial records, including the size of meals and entertainment expenses. Nortek also failed to review or test Linear China's accounts, or to establish procedures to train the subsidiary's employees in anti-corruption compliance. In addition, Linear China's accounting department actively participated in the misconduct when it "in some instances...entered the illicit payments as entries in various accounts and supported the expenditures with false or misleading information and supporting documentation."

a. Self-Reporting, Cooperation, and Remedial Measures

In 2014, an internal audit identified questionable payments in Linear China's books and records, prompting Nortek to conduct an internal investigation of Linear China's misconduct, including through forensic analysis of Linear China's financial records. The investigation confirmed that improper payments had been made to Chinese officials in Shenzhen. Before completing its full investigation, Nortek self-reported its preliminary findings to the SEC and DOJ.

Nortek provided the SEC with comprehensive disclosure of the findings of its investigations, including identifying all improper payments and potentially improper payments made to foreign officials.

The SEC stressed that Nortek assisted the SEC by “effectively segregating, organizing, and presenting the most salient documents to the staff” to make the SEC’s review easier. The SEC noted that Nortek also assisted by making witnesses available—particularly including witnesses located in China—and by providing summaries of witness interviews, voluntarily translated documents, and timely updates of newly discovered information in the course of the internal investigation. Nortek also evaluated its other Chinese businesses to determine whether improper conduct had occurred there as well.

Nortek took immediate actions to end the improper payments and conducted significant remedial measures including the termination of employment of the Linear China managing director and CFO and an extensive review of its compliance program. The SEC highlighted specific corrective steps including: (i) provision of mandatory FCPA and anti-corruption training to its employees across the globe, and in appropriate languages, (ii) strengthening of anti-corruption policies, (iii) development of a compliance committee with representatives from management and subsidiaries to supervise compliance implementation, and (iv) modification of its internal audit schedule to prioritize high-risk geographic locations.

b. DOJ Declination: Factors Cited in Decision Not to Prosecute

The DOJ’s one-page declination letter cited the FCPA Pilot Program and stated that, “despite the bribery by employees of the Company’s subsidiary in China,” the DOJ declined to prosecute Nortek because of a number of factors, including but not limited to:

- The fact that Nortek’s internal audit function identified the misconduct;
- Nortek’s prompt voluntary self-disclosure;
- Nortek’s thorough investigation;
- Nortek’s fulsome cooperation including identifying all involved or responsible individuals and providing all facts relating to that misconduct to the DOJ;
- Nortek’s agreement to continue to cooperate in any ongoing investigations of individuals;
- Nortek’s newly enhanced compliance program and internal accounting controls;
- Nortek’s full remediation, including terminating all five individuals involved in the China misconduct, two of whom were high-level executives of the China subsidiary; and
- Nortek’s disgorgement to the SEC.

18. Novartis

On March 23, 2016, Swiss-based pharmaceutical company Novartis AG (“Novartis”) agreed to pay approximately \$25 million to settle SEC allegations that it violated the books and records and internal accounting controls provisions of the FCPA through the conduct of two of its subsidiaries in China. The SEC Cease and Desist Order (the “Order”) states that Novartis offered, and the SEC had accepted, the settlement in which the company (without admitting or denying any of the findings in the Order) agreed to

disgorge \$21,579,217, pay prejudgment interest of \$1,470,887, and pay a civil penalty of \$2,000,000. Though based in Basel, Switzerland, Novartis is traded on the New York Stock Exchange and employs 120,000 people in 180 countries.

As described in greater detail below, the SEC found that between 2009 and 2013, employees and agents of two Novartis subsidiaries in China used various methods—including false receipts and fake medical studies—to provide money and things of value to Chinese health care providers (“HCPs”) to influence them to favor Novartis products. They would then improperly record these costs as legitimate expenses for conferences, lecture fees, marketing events, educational seminars, and medical studies. The false receipts were used to obtain reimbursement money, which was used to provide improper travel and entertainment to Chinese HCPs as rewards and inducements for prescribing Novartis products.

The settlement appears to have arisen from the results of an internal investigation prompted by whistleblower allegations. In August 2013, one month after the arrest of four GlaxoSmithKline (“GSK”) sales employees in China as part of an investigation into alleged bribery of doctors and healthcare officials, a Chinese newspaper published allegations that Novartis and French drug maker Sanofi S.A. had also engaged in allegedly corrupt activity which bore similarities to the allegations made against GSK.

According to the paper, an unnamed former Novartis employee who supervised drug sales to large Beijing hospitals alleged that she was instructed to pay RMB 50,000 in bribes to doctors in order to obtain RMB 640,000 worth of cancer drug sales during June and July of 2013. At the time, Novartis responded by stating that it had launched an internal investigation into the claims, and added that the whistleblower had threatened Novartis with unspecified actions if the company did not pay her RMB 5,000,000 in compensation. The Chinese government also announced that it would intensify efforts to investigate corruption in the pharmaceutical sector. This prompted speculation among some journalists that Chinese corruption probes were politically motivated—aimed at extracting lower prices from foreign drug makers and/or bolstering China’s domestic pharmaceutical industry.

The SEC Order stated that Novartis conducted an “expansive review” into its relationships with third party travel and event planning vendors. This review, the results of which were shared with the SEC, revealed that that a significant percentage of events did not comply with existing Novartis policies and procedures, including “events for which no record existed to verify it had occurred, events for which inconsistent records existed, and events that could not be verified from available information.”

Employees at one subsidiary, Shanghai Novartis Trading Ltd (“Sandoz China”), provided cash, gifts, entertainment, and favors to HCPs and their family members, with the knowledge of Sandoz China management. Sandoz China employees submitted fake or falsified receipts for reimbursement, and then used the cash to fund gifts and entertainment provided to the HCPs. Certain Sandoz China employees maintained spreadsheets that directly linked certain cash values (referred to as “investments”) paid to HCPs in exchange for a number of monthly Novartis product prescriptions. HCPs were categorized into tiers, including one described by Sandoz China employees as “money worshippers.” The annual “investment” kickbacks ranged from several hundred to several thousand dollars per year per HCP. Sandoz China employees also organized phony medical studies, that were not approved by the Novartis Global Internal Quality Assurance group as are legitimate medical studies, and paid HCPs to collect and

analyze data regarding patient reactions to Novartis drugs. Although no genuine data was collected, payments made under these purported studies totaled approximately \$522,000 between 2009 and 2010.

Besides gifts and cash, Sandoz China employees regularly retained complicit local Chinese travel and event planning companies to pay the travel expenses for HCPs in connection with educational conferences and business events. However, the travel often “did not include an educational purpose or the scientific/educational components were minimal in comparison to the sightseeing or recreational activities, and were instead a method of influencing the HCPs. The related expenses were approved and paid with little or no supporting documentation.” In one case highlighted by the SEC Order, Novartis paid a Chinese travel company \$25,000 for a medical lecture by certain HCPs to educate other HCPs, “despite the lack of any confirmation: (1) that the lecture was organized by Sandoz China and held in the venue for which an invoice was submitted; and (2) that the lecture was attended by HCPs.”

Like Sandoz China, the other Novartis subsidiary named in the Order—Beijing Novartis Pharma Co., Ltd. (“Novartis China”)—organized “thousands” of marketing events through numerous (unnamed) third party travel and event planning vendors that arranged venues, flights, hotels, transit, food and entertainment. Without describing specific examples of conduct, the Order stated that Novartis “did not have sufficient internal accounting controls or anti-corruption compliance measures” in place, failed to conduct adequate due diligence on the third parties, failed to require sufficient proof of services documentation for the expenses submitted by the third parties, and failed to provide adequate anti-corruption training to its personnel with respect to the third party relationships. The Order noted, however, that Novartis had taken prompt remedial measures to improve such control shortcomings, including “overhauling its anti-corruption policies and procedures, terminating and/or imposing other disciplinary sanctions against culpable employees, suspending vendor relationships and payments, doubling its training initiatives, re-organiz[ing] its compliance function to include enhanced oversight by regional and headquarter compliance personnel, and eliminat[ing] the use of vendors to support external meetings.”

The SEC Order contains continuing obligations for Novartis. Although it did not impose an external monitor or compliance consultant, it requires Novartis to provide regular reports to the SEC over the next two years on the progress of its remediation efforts. Specifically, the Order requires Novartis to (1) conduct an initial review and submit an initial report within 180 days of the Order, and (2) conduct and prepare two follow-up reviews and reports within 270 days, and 450 days respectively, of completion of the initial report. The Order also requires Novartis to certify its compliance with the SEC undertakings, providing sufficient support to evidence such compliance.

At press time, media reports indicated that over 25 individuals are also facing legal repercussions in South Korea for conduct similar to that which is described above in China. Korean authorities raided Novartis Korea’s offices in Seoul in February 2016, and the subsidiary’s first Korean CEO, Moon Hak-sun, was suspended from all duties in April 2016. Then, on August 8, 2016, South Korean prosecutors indicted six current and former Novartis Korea executives, including Moon, principally on charges that they paid more than \$2.3 million in bribes to doctors through a program of academic events sponsored by trade journals in exchange for prescriptions of Novartis products. Reportedly, the Seoul Western District Prosecutor’s Office also indicted six medical journal publishers and fifteen doctors on related charges. According to a spokesman for Novartis, South Korean prosecutors have asked the government to suspend Novartis’ operations in the country. In a statement reported by the press, Novartis admitted

some improper conduct, acknowledging that “certain associates in Korea conducted small medical meetings . . . through trade journals, in violation of our policies . . . [and] some associates supported travel to overseas congresses for some healthcare practitioners in a way that did not fully comply” with standards of self-regulation established by the Korean Research-based Pharma Industry Association.

In the United States, Novartis is also facing charges in the Southern District of New York that it provided U.S. HCPs with kickbacks worth more than \$65 million in cash and entertainment. In *United States v. Novartis Pharmaceuticals Corp.*, the Department of Justice is alleging that Novartis violated the Anti-Kickback Statute by paying HCPs honoraria that, in some cases, amounted to tens of thousands of dollars per doctor, to speak at more than 38,000 Novartis-funded speaking events. The Department of Justice alleges that these speaking events, held at high end restaurants, sports bars, Hooters restaurants, and fishing lodges, were excuses to bribe HCPs with cash and lavish dinners. Novartis employees, according to the Department of Justice allegations, also recorded numerous sham speaking events and paid honoraria for the HCPs even though those events did not occur and no HCPs attended.

19. NuSkin

On September 20, 2016, the SEC filed an order instituting cease-and-desist proceedings against Nu Skin Enterprises, Inc. (“Nu Skin”) for violations of the FCPA’s accounting and internal controls provisions. Nu Skin, a publicly-traded Delaware corporation based in Utah, manufactures and markets personal and nutritional supplement packets. Nu Skin consented to the SEC’s Order, without admitting or denying the SEC’s allegations, and agreed to pay \$765,688 (comprising disgorgement of \$431,088, prejudgment interest of \$34,600, and a civil money penalty of \$300,000).

The SEC’s allegations center on the activity of Nu Skin’s wholly-owned Chinese subsidiary, Nu Skin (China) Daily Use & Health Products Co. Ltd. (“Nu Skin China”). Under China’s Direct Selling Laws, Nu Skin China was required to obtain a direct selling license from the national, provincial, and local levels prior to operating in any particular Chinese city. According the SEC, in 2013 Nu Skin China held a promotional event in a city in which it did not have the required licenses. The relevant province’s Administration of Industry and Commerce (“AIC”) subsequently investigated the Nu Skin China promotional event and informed Nu Skin China that it intended to charge Nu Skin China and certain sales staff with violations of the Direct Selling Laws.

According to the SEC Order, Nu Skin China anticipated that an action by the AIC would have an adverse impact on Nu Skin China’s long-term business development. As a result, Nu Skin China approached an official of the Communist Party in China who had previously served as a supervisor to the provincial head of the AIC. Nu Skin China allegedly asked that the Party Official intervene with the AIC investigation and charging decision. In return, Nu Skin China allegedly offered to make a 1,000,000 RMB (approximately \$154,000) donation to a charity associated with the Party Official.

The SEC’s Order indicates that Nu Skin China informed Nu Skin of the proposed donation, but failed to disclose the connection of the donation to the AIC investigation. Nu Skin instructed Nu Skin China to consult with external U.S. legal counsel to ensure the contribution complied with the FCPA. Nu Skin China’s retained counsel advised Nu Skin China to incorporate FCPA contractual provisions in the donation agreement. According to the SEC, although a draft of the donation agreement included FCPA

provisions, the provision were ultimately removed from the final version. Nu Skin was unaware that the anti-corruption language was removed from the final agreement.

A week after executing the donation agreement, Nu Skin China held a donation ceremony in the relevant province. The Party Official, a top official from the AIC, and a representative of Nu Skin China all attended the ceremony. Two days later, Nu Skin China received notice that the AIC had determined not to charge or fine Nu Skin China.

According to the SEC, Nu Skin China's internal expenditure authorization form inaccurately described the purpose of the donation as charitable rather than as a payment to influence the Party Official. As a result, the SEC alleged that Nu Skin violated FCPA's books and records provisions, which require issuers to maintain books and records that accurately and fairly reflect the transactions and disposition of the assets of the issuer. The SEC also alleged that Nu Skin violated the internal controls provisions of the FCPA. In particular, the SEC alleged that Nu Skin failed to ensure that adequate due diligence was conducted with respect to charitable donations in China, despite knowing the corruption risks in China.

20. Och-Ziff

On September 29, 2016, Och-Ziff Capital Management Group, LLC ("Och-Ziff"), a New York-based hedge fund, agreed to pay \$412.1 million to the DOJ and SEC to resolve allegations that it violated the FCPA and securities laws in a number of African countries between 2007 and 2013.

The DOJ charged Och-Ziff with two counts of conspiracy to violate the anti-bribery provisions of the FCPA, one count of violating the books and records provisions, and one count of violating the internal controls provisions. Och-Ziff resolved these charges through a three-year deferred prosecution agreement under which it agreed to pay a criminal penalty of slightly more than \$213 million, implement rigorous internal controls, retain an independent compliance monitor for three years, and cooperate with the DOJ's ongoing investigation. Och-Ziff's subsidiary, OZ Africa Management GP LLC ("OZ Africa"), pleaded guilty to a one-count criminal information charging OZ Africa with conspiracy to violate the anti-bribery provisions of the FCPA.

The SEC filed claims against Och-Ziff for violating the anti-bribery provisions, books and records provisions, and internal controls provisions of the FCPA. The SEC also filed claims against OZ Management LP ("OZ Management"), an Och-Ziff subsidiary, for violating the Investment Advisers Act. Och-Ziff and OZ Management settled these claims and agreed to pay disgorgement of just over \$173 million. Och-Ziff also agreed to retain an independent compliance monitor for three years and implement enhanced compliance controls.

a. DOJ and SEC Allegations

According to the DOJ and SEC, between 2007 and at least 2013, Och-Ziff and its subsidiaries and joint venture partners entered into a series of transactions and investments in which they paid bribes through intermediaries, agents, and business partners to government officials in Libya, the Democratic Republic of Congo (DRC), Chad, Niger, the Republic of Congo, and Guinea, amongst other places. The DOJ and SEC alleged that Michael Cohen, former head of Och-Ziff's London office, and Vanja Baros, a

former analyst in the private investments group at Och-Ziff's European office and a member of the firm's African Special Investment Team, had actual knowledge of the bribe payments and other misconduct. The charging documents also indicate that numerous other Och-Ziff employees, including Och Ziff's founder and CEO, Daniel Och, ignored red flags and the Company's own internal policies and procedures when permitting high-risk transactions to proceed.

Although the DOJ and SEC charges touch upon conduct and lack of internal controls in a number of African countries, the anti-bribery violations focus mainly on Och-Ziff's investments in the DRC and Libya.

i. Conduct in the Democratic Republic of Congo

In the DRC, Och-Ziff entered into a partnership with an Israeli businessman to pursue various mining assets. The Israeli businessman is widely reported by U.S. and international press to be Dan Gertler, a businessman with close ties to the family of the President of the DRC. Although not identified in the charging documents per the usual practice of the DOJ and SEC, this summary will refer to Mr. Gertler by name for ease of reference and because Mr. Gertler has been so widely reported to be the individual referenced in the charging documents.

Cohen and Baros began discussions with Gertler in 2007 or 2008 regarding the formation of a joint venture to create a large mining company in the DRC. Gertler, who Och-Ziff knew had access to attractive investment opportunities in DRC, explained to Cohen and Baros that he would need to pay substantial bribes to DRC officials for access to the investments and that he expected Och-Ziff to fund these bribe payments. Other Och-Ziff personnel, including Daniel Och and CFO Joel Frank, ignored certain red flags and company procedures when approving various aspects of this partnership.

As an initial step in the partnership with Gertler, Och-Ziff, OZ Africa, or Africa Global Capital ("AGC") (an investment fund established by an Och-Ziff joint venture) funded investments into two companies owned or controlled by Gertler with an eye toward acquiring mining assets in DRC. First, in 2008, Och-Ziff purchased approximately \$150 million worth of shares in a publicly-traded mining company controlled by Gertler (referred to in the DPA as "Company A"). Och-Ziff and Gertler planned for Company A to acquire a majority stake in Africo Resources Ltd., a Canadian mining company that owned copper assets in the DRC in close proximity to a mine controlled by Gertler. The plan was for Och-Ziff to also invest in Gertler's mine and for the parties to ultimately merge the assets under Company A.

At the time, Africo was engaged in a dispute with a Congolese mining company called Akam Mining SPRL ("Akam"). The dispute had led to the seizure by the DRC government of another copper mine owned by Africo. According to the DOJ, this seizure had in fact been orchestrated by a DRC official. The same day that Och-Ziff agreed to purchase \$150 million worth of Company A, Gertler caused \$11 million to be delivered to this DRC official.

In order to obtain control of important mining rights, Och-Ziff and AGC provided a convertible loan of approximately \$124 million to another company controlled by Gertler (referred to in the DPA as "Company B"). Company B used the funds to purchase Akam, make a shareholder loan to Africo, and pay additional bribes to DRC officials. Shortly after the shareholder loan from Company B, Africo announced that it had reached an agreement with Company B for Company B to purchase 60% of

Africo's shares, pending approval by Africo's shareholders. In order to ensure approval by the shareholders, Gertler bribed DRC officials, including judges, to make sure that Africo did not obtain a favorable ruling in the pending case with Akam. As a result, Africo lost its interest in the mine and Company B's acquisition was approved.

According to the DOJ, Och-Ziff and AGC did not exercise the option to convert their loan into equity in Company B and instead continually extended the repayment dates for the convertible loan until a publicly traded mining company purchased Company B. In order to attract this buyer and obtain a favorable price, Gertler bribed DRC officials to obtain additional mining assets for Company B. Among the additional assets obtained by Gertler for Company B were assets that had been recently seized by the DRC government and were sold to Gertler at a significant discount. The mining company ultimately acquired a 50.5% stake in Company B and agreed to repay the loan to Och-Ziff and AGC.

After the sale of a majority interest in Company B, Och-Ziff provided additional financing to fund Gertler's activities in DRC through a margin loan to Gertler totaling \$130 million. Following the death of a DRC official closely linked to Gertler, Och-Ziff began winding up its business with Gertler. In total, according to the DOJ, Gertler paid or caused to be paid more than \$100 million in bribes to DRC officials to obtain special access, discounted prices, or other advantages in obtaining mining rights in the DRC. Och-Ziff sold off its positions and received payments on its loans, earning a profit of approximately \$91 million from its business with Gertler.

According to U.S. authorities, Och-Ziff was aware of the significant risks involved in working with Gertler from the outset of the relationship. Och-Ziff ignored these risks, at least in part at the direction of Daniel Och. In early February 2008, when Och-Ziff was first contemplating partnering with Gertler, Och-Ziff obtained a background report on Gertler as required by its anti-corruption policy. The report noted that Gertler had used his political influence in the DRC to facilitate his business dealings and was considered a politically exposed person given his close ties to high-ranking DRC officials. In response to this report, a number of Och-Ziff personnel, including Joel Frank and Och-Ziff's then-chief legal officer, expressed concern about the proposed partnership. According to the SEC, Daniel Och ultimately instructed employees to move forward with the relationship. Additionally, in 2008, employees in the DRC conducted an audit of the convertible loan provided by Och-Ziff and AGC to Company B. The auditors initially indicated in their report that they could not get satisfactory answers from Gertler's employees regarding certain expenses for which the loan funds were used and indicated that the expenses were likely for maintaining "political alignment" and "protocol" with the authorities in DRC. According to the DOJ, Baros instructed the auditors to remove this language from their report. The DOJ and SEC noted a number of other significant red flags that were either wholly ignored by Och-Ziff or not properly addressed.

ii. Conduct in Libya

In Libya, Och-Ziff engaged a third party agent to assist Och-Ziff in securing an investment from the Libya Investment Authority. According to the SEC, Cohen was largely responsible for initiating and overseeing these efforts and was aware that the third party agent would make improper payments to Libyan officials to secure the investment.

Cohen and the third-party agent agreed that the agent would receive a fee of \$3.75 million based on an investment from the Libya Investment Authority of \$300 million. After receiving the investment, Och-Ziff paid the agency fees to a special purpose vehicle set up by the agent in the British Virgin Islands. After each payment, the agent allegedly transferred money to accounts held by, or for the benefit of, high-ranking Libyan officials. Och-Ziff ultimately earned a total of more than \$100 million in fees and incentive income from the Libya Investment Authority's business.

During the time that the agent was working as Och-Ziff's intermediary, Och-Ziff also invested \$40 million in a Libyan real estate development project that was founded and overseen by the agent. Government officials, including a daughter of then-Libyan President Muammar Gaddafi, had interests in this project. In connection with this investment, Och-Ziff paid a \$400,000 "deal fee" to an entity controlled by the Libyan agent, which Cohen allegedly knew would be used to compensate the agent for bribes paid in connection with the development project.

b. Lack of Internal Controls

The DOJ and SEC made clear that, despite doing business in countries with high corruption risks, including the DRC, Libya, Chad, and Niger, Och-Ziff failed to implement an adequate system of internal accounting controls and failed to enforce the controls it did have in place. In particular, Och-Ziff failed to maintain controls over the retention and monitoring of third parties. For example, in Chad and Niger, an AGC portfolio company used funds provided by Och-Ziff to pay a Gabonese consultant a fee that was nearly two and half times the salary of any of the portfolio company employees. The consultant was Samuel Mebiame, the son of a former Prime Minister of Gabon. Despite learning that the portfolio company's payments to Mebiame were not adequately justified, Och-Ziff continued to fund capital calls for the portfolio company in the amount of more than \$20 million. Och-Ziff even continued to do business with Mebiame after he refused to sign anti-corruption warranties. According to the DOJ, Mebiame paid at least \$2 million in bribes to government officials in Niger and Chad in connection with obtaining uranium concessions for the portfolio company.

c. Charges Against Individuals

A number of individuals have also been subject to enforcement in connection with Och-Ziff's misconduct. The SEC charged Daniel Och with violating the FCPA's books and records provisions. The SEC also charged Joel Frank with violating the books and records and internal controls provisions. The SEC alleged that Och personally approved two transactions in the DRC in which bribes were paid and then inaccurately recorded on Och-Ziff's books and records. The SEC alleged that Frank approved the expenditure of funds in transactions in which bribes were made in the DRC and Libya. According to the SEC, although neither Och nor Frank knew that bribes would be paid, they were aware of the high risk of corruption in transactions and caused Och-Ziff's books and records violations by approving and authorizing such transactions. Och was required to pay disgorgement of \$1.9 million and prejudgment interest of \$273,718 for a total penalty of over \$2.1 million. Frank was not required to pay a monetary penalty, but agreed to cooperate with the SEC's investigation and refrain from committing or causing further violations of the FCPA. Neither Och nor Frank admitted or denied the SEC's findings.

On January 26, 2017, the SEC filed claims against Cohen and Baros. On May 29, 2017, the SEC filed an amended complaint against Cohen and Baros. The SEC alleged that Cohen and Baros

orchestrated Och-Ziff's bribery in Libya, Chad, Niger, Guinea, and the DRC. The SEC claims that Cohen and Baros violated the anti-bribery provisions of the FCPA, violated the internal controls provisions of the FCPA, aided and abetted Och-Ziff's violations of the anti-bribery provisions and the books and records provisions, and aided and abetted OZ Management's violations of the Investment Advisors Act. The SEC also claims that Cohen violated the Investment Advisors Act. Both Cohen and Baros have moved to dismiss the claims against them, arguing that the claims are time-barred, involve improper extraterritorial application of the Investment Advisors Act, and fail to allege the requisite knowledge of improper conduct on the part of Cohen and Baros. As of the date of publication, the case is pending.

Mebiame pled guilty to conspiracy to violate the anti-bribery provisions of the FCPA for his role in facilitating bribe payments in Niger and Chad. On May 31, 2017, he was sentenced to two years in prison. Although Mebiame is a dual citizen of Gabon and France, the DOJ alleged that he took numerous steps while in the United States in furtherance of the corrupt scheme, including exchanging email and other communications with co-conspirators, receiving payments related to the scheme in U.S. bank accounts, and meeting with co-conspirators to discuss the corrupt scheme.

21. Odebrecht and Braskem

On December 21, 2016, Odebrecht S.A. ("Odebrecht"), a Brazil-based construction and engineering conglomerate with global operations, pleaded guilty in the United States District Court for the Eastern District of New York to one count of conspiracy to violate the FCPA's anti-bribery provisions. In related proceedings, Odebrecht also entered into settlements with the Ministerio Publico Federal in Brazil and the Office of the Attorney General in Switzerland. Odebrecht admitted to paying approximately \$788 million in bribes over the course of 15 years in 12 countries including Angola, Argentina, Brazil, Colombia, Dominican Republic, Ecuador, Guatemala, Mexico, Mozambique, Panama, Peru and Venezuela.

Odebrecht agreed that a criminal fine of \$4.5 billion was appropriate but argued that it was unable to pay more than \$2.6 billion. Following an ability to pay analysis, at Odebrecht's sentencing hearing on April 17, 2017, U.S. District Judge Raymond J. Dearie of the Eastern District of New York signed off on a criminal penalty of \$2.6 billion. The DOJ agreed that this amount would be offset by any amount Odebrecht paid to Brazil and Switzerland through their respective agreements. Ultimately, Odebrecht will pay \$2.39 billion to Brazil, \$116 million to Switzerland, and \$93 million to the United States.

In a separate but related proceeding, a partially-owned Odebrecht subsidiary, Braskem S.A. ("Braskem"), also pleaded guilty to one count of conspiracy to violate the FCPA's anti-bribery provisions. Braskem, headquartered in Brazil with ADRs traded on the New York stock exchange, was the largest petrochemical company in the Americas. Braskem's largest shareholders are Odebrecht and Brazil's state-controlled oil company, Petrobras. Braskem also entered into settlements with the SEC, the Ministerio Publico Federal in Brazil and the Office of the Attorney General in Switzerland. Braskem admitted to paying at least \$75 million in bribes to government officials in Brazil, including Petrobras employees. As part of its plea agreement, Braskem agreed to pay a criminal penalty of \$632.6 million. Braskem agreed to pay fifteen percent of the penalty (approximately \$94 million) to the U.S., 15% to Switzerland, and the remaining 70% (approximately \$442 million) to Brazil. Braskem also agreed to pay disgorgement in the amount of \$325 million (\$65 million to the SEC and the remaining \$260 million to Brazilian authorities).

a. Odebrecht's "Department of Bribery"

Founded in the 1940s by engineer Norberto Odebrecht, Odebrecht expanded to become one of the largest construction conglomerates in Latin America. To fuel this expansion, Odebrecht, under the management of Norberto's grandson Marcelo Odebrecht, engaged in bid-rigging and the bribery of Brazilian and foreign officials from roughly 2001 onward. In 2006, Odebrecht began to approach these corrupt practices in a systematic, organized fashion. Odebrecht created a department within Odebrecht subsidiary Construtora Norberto Odebrecht ("CNO") called the Division of Structured Operations ("DSO"), which Deputy Assistant Attorney General Sung-Hee Suh of the DOJ Criminal Division referred to as the "Department of Bribery." Over a fifteen-year period, Odebrecht paid more than \$788 million in bribes to government officials and executives of state-owned companies. These illegal payments were managed and disbursed in large part via the DSO and resulted in over \$3.36 billion in ill-gotten gains.

The DSO oversaw Odebrecht's "shadow" budget dedicated to bribery. To conceal its activities, the DSO used an off-book computer system to process and track illegal payments. The DSO also used a separate communications system to exchange secure emails and instant messages among members of the DSO and with outside co-conspirators. In order to fund its illegal payments, Odebrecht generated money that was never disclosed in its financials or on its balance sheets by, for example, charging subsidiaries overhead fees, omitting its service provider charges from project budgets, and failing to declare commissions for company asset purchases. The DSO then funneled Odebrecht's unrecorded funds to off-shore entities—also not disclosed on the company's balance sheets—that were set up by the DSO and managed by proxy executives. Most of the illegal payments were funneled through up to four layers of off-shore entities before reaching the final recipient.

Off-shore banks also played a central role in Odebrecht's payment scheme. Odebrecht preferred to use small banks located in countries with strong banking privacy laws, such as the Antigua Overseas Bank. Later, Odebrecht even went so far as to purchase a controlling share of the Antiguan branch of an Austrian bank, Meinl Bank, when the branch was failing. These off-shore banks provided accounts both for Odebrecht's off-shore entities and for recipients of Odebrecht's bribes.

In addition to elaborate bank transfers schemes, Odebrecht also resorted to cash bribes, both inside and outside of Brazil, using secret package or suitcase drop-offs in specified locations. For example, a Chinese *doleiro* nicknamed "Dragon" reportedly routinely delivered packages of cash in an armored car at the heart of Sao Paulo's busy shopping district.

While much of Odebrecht's illegal scheme took place outside of the United States, Odebrecht and the DSO also committed overt acts in or involving the United States, bringing Odebrecht under the jurisdiction of the DOJ. For example, starting in 2006, Odebrecht transferred funds totaling more than \$100 million from several unnamed New York bank accounts to the accounts of Odebrecht's off-shore companies

Once Odebrecht learned it was under scrutiny, several Odebrecht and DSO executives attempted to conceal or destroy evidence to obstruct the ongoing investigations. For example, Odebrecht agreed to pay \$4 million in bribes to high-level Antiguan officials in exchange for their refusal to hand over inculpatory banking documents to authorities. Odebrecht executives further instructed employees to

delete emails and records and to destroy encryption keys in order to permanently block access to its off-book computer system.

b. Corrupt Payments

i. *Corrupt Payments in Brazil*

Nearly half of Odebrecht's illegal payments were made in Brazil to Brazilian political parties, government officials, and executives of state-owned companies. According to the DOJ, bribe payments totaling over \$349 million were made in Brazil, generating estimated ill-gotten benefits of over \$1.9 billion.

Much of the corrupt payment scheme in Brazil focused on Petrobras. In connection with its Petrobras business, Odebrecht participated in a cartel with other construction companies (the "Cartel Companies"). The Cartel Companies evaluated and divided up future Petrobras contracts. To ensure that the contracts were awarded to the appropriate company, other Cartel Companies submitted intentionally disqualifying bids, and paid bribes to Petrobras officials aware of the scheme. For example, in 2010, the Cartel Companies agreed that Odebrecht would win a Petrobras contract to provide environmental and security certification services. In order to secure the contract, Odebrecht paid more than \$40 million from the DSO to Brazilian political parties. Certain of these funds were ultimately directed to specific Brazilian government officials.

Odebrecht also used the DSO to pay bribes to political parties, candidates for office, and other local and national government officials to obtain other non-Petrobras business in Brazil. For example, between 2011 and 2014, Odebrecht used the DSO to pay bribes totaling approximately \$9.7 million to a Brazilian political party at the request of a high-ranking official within the legislative branch in order to secure the political party's influence to continue a construction project on which Odebrecht ultimately earned profit of more than \$140 million. In another instance, Odebrecht used the DSO to pay a high-level state elected official approximately \$20 million in order to obtain and retain business on a transportation project.

ii. *Corrupt Payments Outside of Brazil*

Odebrecht's illegal behavior, however, was not limited to Brazil. Odebrecht paid or caused to be paid more than \$430 million in bribes to foreign officials or foreign political parties outside of Brazil including Angola (\$50 million over at least seven years), Argentina (\$35 million over at least seven years), Colombia (\$11 million over at least five years), the Dominican Republic (\$92 million over at least 13 years), Ecuador (\$33.5 million over at least nine years), Guatemala (\$18 million over at least two years), Mexico (\$10.5 million over at least four years), Mozambique (\$900,000 over at least three years), Panama (\$59 million over at least four years), Peru (\$29 million over at least nine years), and Venezuela (\$98 million over at least nine years). The schemes largely followed a familiar pattern, with Odebrecht using unrecorded funds from the DSO to make payments directly to government officials or to third party intermediaries with the understanding that such payments would be paid to government officials. In return, Odebrecht secured lucrative infrastructure and public works contracts in the countries, obtained favorable terms in ongoing negotiations, influenced the allocation of government resources, and resolved issues that arose in ongoing projects.

For example, in Venezuela, Odebrecht generally relied on intermediaries to negotiate with government officials. Odebrecht understood that the intermediaries, who were paid a percentage of the contract price as compensation, would bribe these government officials to influence the award of contracts, obtain confidential pricing information, and exert influence over the allocation of government resources to projects in which Odebrecht had an interest.

c. Braskem Conduct

Between 2002 and 2014, Braskem authorized bribes to Brazilian politicians, political parties, and a Petrobras official in order to reduce Braskem's tax liabilities, help Braskem maintain a joint venture with Petrobras, and obtain a reduction in the price of raw materials Braskem purchased from Petrobras. To conceal its payments, Braskem provided funds to Odebrecht's DSO, which were then sent through a series of offshore entities before being paid to relevant officials.

Around 2006, in response to judicial rulings that put at risk lucrative tax credits from which Braskem benefited, Braskem and Odebrecht began a multi-year campaign to obtain legislative action to preserve the tax credits. As part of these efforts, Braskem agreed to make a contribution of R\$50 million (approximately \$32 million) to the political campaign of a Brazilian politician, knowing that the funds would not be used for the campaign but rather divided among several Brazilian politicians. Braskem made the payment through the DSO and legislation was ultimately passed effectively preserving the benefit from the tax credit. Braskem's plea agreement details several other instances in which Braskem corruptly paid national and local officials, candidates for office, or political parties through DSO in order to obtain favorable tax treatment.

Braskem also paid millions of dollars in bribes in connection with its business with Petrobras. For example, in 2005, Braskem agreed with Petrobras to form a joint venture to build a polypropylene plant. When public pressure against the plant caused Braskem executives to worry that Petrobras might back out of the agreement, Braskem bribed a Petrobras executive and a Brazilian congressman so that the officials would exercise their influence to ensure that Petrobras honored the contract. Between 2007 and 2008, Braskem paid the officials R\$4.3 million (approximately \$3.1 million under then-existing exchange rates). In another instance, Braskem paid the same two individuals a total of \$12 million in bribes to intervene in ongoing negotiations between Braskem and Petrobras regarding a long-term supply contract for naphtha, a raw material Braskem used in petrochemical operations. As a result of the officials' intervention, Braskem was able to obtain more favorable pricing on naphtha.

d. Odebrecht and Braskem Fall-Out

Numerous individuals at Odebrecht, up to and including former CEO Marcelo Odebrecht, were convicted and jailed in the wake of the investigations. In March 2016, a Brazilian federal court sentenced Marcelo Odebrecht to 19 years in prison for money laundering, corruption, and involvement in a criminal association. However, in exchange for his cooperation with authorities, Marcelo Odebrecht's sentence was reportedly reduced to two and a half years in prison, followed by five years of house arrest. As of a March 7, 2017 report, a total of 76 other Odebrecht executives have also been jailed.

The taint of the Odebrecht bribery scheme also reached a number of high-level politicians, both within and outside of Brazil, rooted out with the assistance of cooperating witnesses. Within Brazil, the scandal has reached the highest level of the government, resulting in charges against the last three

presidents of Brazil. The cases against these individuals and other Brazilian government officials are discussed in detail in Chapter 4.

Outside of Brazil, the Odebrecht scheme has implicated dozens of Latin American politicians and legislators. Alejandro Toledo, president of Peru from 2001 to 2006, is currently wanted by the Peruvian government for accepting \$20 million in corrupt payments from Odebrecht. With Toledo presumed to be in hiding in California, Peru's current president Pedro Kuczynski requested that U.S. President Trump extradite Toledo to stand trial in Peru. Kuczynski himself is also under investigation alongside two other former Peruvian heads of state for possible ties to Odebrecht. Additionally, Interpol has issued warrants for the arrest of two sons of Panama's former president, Ricardo Martinelli. Panama's current president, Juan Carlos Varela, is also under scrutiny for allegedly accepting Odebrecht money for his political campaign. Investigations and accusations regarding the Odebrecht scheme have also spread to Chile, Colombia, the Dominican Republic, Mexico, and Venezuela.

e. Terms of the Plea Agreement

Despite the scope of Odebrecht's bribery scheme, its failure to voluntarily disclose the violations to regulators, and its initial efforts to obstruct investigators, the DOJ recommended a 25% discount off the bottom end of the Sentencing Guidelines fine range. Twenty-five percent is the maximum reduction allowed under current DOJ guidelines for companies that fail to voluntarily disclose the violation. According to the DOJ, the 25% reduction reflects Odebrecht's full cooperation with the investigation and its "extensive remedial measures." Those remedial measures included termination of 51 employees, discipline and anti-corruption training for a further 26 employees, and the strengthening of anti-corruption measures at the company by appointing a Chief Compliance Officer, adopting more stringent compliance and internal controls processes, and significantly increasing both the human and monetary resources devoted to compliance.

Braskem's \$632 million criminal penalty represents a 15% discount off the bottom of the applicable Sentencing Guidelines fine range. Unlike Odebrecht, Braskem received only partial credit for its cooperation with the DOJ investigation. Braskem failed to receive full cooperation credit because it did not start cooperating until the DOJ had developed significant evidence on its own. The DOJ noted Braskem's significant remedial measures, particularly the wholesale enhancements made to its anti-corruption compliance program.

Under the terms of their respective plea agreements, Odebrecht and Braskem each agreed to retain corporate compliance monitors for a period of three years.

22. Olympus

a. Overview

On February 29, 2016, as part of a coordinated enforcement action, the medical imaging and surgical equipment company Olympus entered into several settlements and agreements to resolve criminal charges and civil claims relating to violations (and/or conspiracies to violate) the FCPA, the Anti-Kickback Statute ("AKS") as well as the federal False Claims Act ("FCA") and state FCA statutes. In total, Olympus agreed to pay \$646 million and entered into two separate DPAs with the DOJ, a civil settlement,

as well as a “Corporate Integrity Agreement” with the Office of Inspector General of the U.S. Department of Health and Human Services (“HSS Department”).

Olympus Corporation (“Olympus”) is a Japanese-incorporated company with operations across the globe. The settlements of the above-mentioned coordinated enforcement action were entered into not with Olympus, but with two U.S.-based subsidiaries of Olympus: (i) Olympus Corporation of the Americas (“OCA”), a New York corporation headquartered in Pennsylvania, which oversees operations in all of the Americas and (ii) Olympus Latin America Inc. (“OLA”), a Delaware-incorporated subsidiary headquartered in Miami, in charge of overseeing operations in the Caribbean and Central and South America. OLA is a subsidiary of OCA.

OLA entered into a three-year DPA with the DOJ and paid \$22.8 million in penalties to resolve charges of violating and conspiring to violate the FCPA’s anti-bribery provision (“OLA DPA”). OLA admitted and accepted as true the facts set out in the OLA DPA, highlights of which are described below. OCA, in its role as OLA’s parent company, agreed to certain terms of the OLA DPA. Importantly, OCA agreed, via the OLA DPA, to enhance its corporate anti-corruption compliance program through various measures, including by conducting periodic risk-based reviews and establishing an effective internal reporting system.

OCA also entered into its own three-year DPA with the DOJ and agreed to pay \$312.4 million in penalties (*i.e.* \$306 million plus accrued interest) to resolve criminal charges that it conspired to violate the AKS, which prohibits exchanging or offering to exchange anything of value to induce (or subsequently reward) the referral of federal health care program business (“OCA DPA”). Again, OCA admitted and accepted as true the facts described in the OCA DPA, summarized below.

Both the OCA and OLA DPAs impose a three-year monitorship by an independent monitor, whose obligations are the same in both monitorships.

In parallel to the resolution of the criminal charges via the DPAs, OCA also settled civil charges under the federal FCA and various state FCA statutes (“Civil Settlement”), pursuant to which OCA agreed to pay an additional \$310.8 million (\$306 million plus interest). The FCA *qui tam* complaint which led to the litigation resolved by the Civil Settlement had been filed by OCA’s former compliance officer, John Slowik. Slowik received approximately \$50 million as part of the Civil Settlement. The Civil Settlement specifies that except for the facts admitted as part of the OCA DPA, the Civil Settlement should not be viewed as an admission of liability by OCA.

OCA entered into the Civil Settlement with, amongst others, the Office of Inspector General of the HSS Department, with whom OCA also entered into a separate five-year Corporate Integrity Agreement. The Corporate Integrity Agreement, which was executed as a condition of release from other administrative sanctions, imposes a wide range of enhancement measures to OCA’s compliance program as relating to federal health care program requirements.

b. Foreign Bribery: FCPA Violations described in OLA PDA

According to OLA DPA, employees of OLA made “hundreds of unlawful payments” and provided “personal benefits, including cash, money transfers, personal or non-Olympus medical education travel, free or heavily discounted equipment, and other things of value” to healthcare professionals employed at

various publicly owned health care facilities in Brazil, Bolivia, Colombia, Argentina, Mexico, and Costa Rica. These direct and indirect payments were made so that the health care professionals would “authorize or influence [the health care] facilities’ decisions to purchase Olympus equipment and to prevent public institutions from purchasing or converting to the technology of competitors.” In total, the unlawful payments made by OLA amounted to approximately \$3 million and generated around \$7.5 million in profits between 2006 and 2011.

The bribery scheme employed by OLA had been devised by OLA’s senior management. OLA identified health care professionals who sat on public tender boards and/or who otherwise had a strong influence over the health care institutions’ purchasing decisions and labeled them as “Key Opinion Leaders” (or “KOLs”). Most of the improper benefits to the KOLs were channeled through specifically established training centers. Although the training centers were apparently also used for legitimate training purposes, their main purpose was to provide pecuniary benefits to the KOLs who managed them. Specifically, in exchange for managing the training centers, KOLs would receive an “annual salary of \$65,000 . . . , a 50% discount on Olympus equipment, and a \$130,000 budget for what was termed ‘VIP Management.’”

Moreover, OLA created a so-called “Miles Program” which provided free travel to KOLs and their family members for non-training center related reasons. Under the program, one “mile” was equivalent to one U.S. dollar that could be used for personal travel expenses. In certain cases, KOLs received as much as 5,000 and 30,000 miles (*i.e.*, \$5,000 and \$30,000).

OLA also maintained a spreadsheet to calculate the “return on investment” and track the sales that could be attributed to KOLs, connecting the value of benefits provided to them.

Numerous emails by OLA employees unequivocally established the expected quid-pro-quo nature of the arrangements. In exchange for the benefits received, KOLs were expected to steer tenders in OLA’s favor. In one particularly candid email, an OLA employee emailed a colleague about a corrupt payment to a health care professional, stating: “[I]t is important for [the health care professional] to understand that what we are doing is not because we are nuns from Mother Teresa’s order in Calcutta. Rather, we expect reciprocity on his part”

OLA tried to cover up the bribery scheme by, *inter alia*, purposefully omitting references to the underlying economic arrangements from relevant contracts. For example, in relation to a donation made to influence a KOL based in Honduras, an OLA employee emailed the following instructions to a local distributor (as translated): “The document should make no allusion (mention, comment, etc.) to the fact that the donation to be made, will favor or promote new business with Olympus or with [the distributor]. The donation should not be interpreted as an action which conditions business later. . . . This is extremely important. I’ll explain in detail later.”

The OLA DPA calculated the base penalty for the above-described conduct at USD 28.5 million, but OLA received a 20% credit for its cooperation with the DOJ, including for having conducted an extensive internal investigation, translating numerous documents, and organizing voluminous evidence. OLA had also taken remedial actions by “terminating its involvement with numerous responsible parties, including employees and third-party distributor relationships in Latin America, and enhancing its due diligence for third-party agents and consultants.”

c. Domestic Bribery: AKS Violations described in OCA DPA

While the OLA-DPA focused on the foreign bribery violations, the OCA DPA settled violations of the AKS. According to the Statement of Facts of the OCA DPA, OCA “sought to, and did, induce doctors, hospitals, and other health care providers to buy OLYMPUS products by giving them various types of remuneration, including grants, payments for travel and recreational activities, consulting payments, and gifts or no-charge loans of OLYMPUS equipment, some of which sold for \$20,000 or more.” Through this conduct, OCA facilitated “more than \$600 million in sales of OLYMPUS medical and surgical equipment” making “more than \$230 million in gross profits.”

23. PTC

On February 16, 2016, the SEC issued an administrative cease-and-desist order against Massachusetts-based technology company PTC Inc. (“PTC”) in connection with allegations that PTC’s wholly-owned Chinese subsidiaries—Parametric Technology (Shanghai) Software Company Ltd. and Parametric Technology (Hong Kong) Ltd. (collectively, “PTC China”), which operated as a single company during the relevant period—violated the anti-bribery, books and records and internal controls provisions of the FCPA. On the same day, PTC China entered into a non-prosecution agreement (“NPA”) with the DOJ to resolve allegations related to this same conduct. As part of its settlement with the SEC, PTC agreed to disgorge profits of \$11,858,000 and pay \$1,764,000 in prejudgment interest; under its NPA with the DOJ, PTC China agreed to pay a penalty of \$14,540,000. The DOJ noted that PTC received partial cooperation credit but did not receive credit for voluntary disclosure because, although PTC had made a disclosure in 2011 in connection with an internal review, it apparently “did not voluntarily disclose relevant facts known to PTC Inc. at the time of the initial disclosure....”

Also in connection with this conduct, the SEC in late 2015 entered into its first-ever deferred prosecution agreement (“DPA”) with an individual (discussed separately below). The three-year DPA was agreed with Yu Kai Yuan, a former employee of PTC China, in exchange for his “significant cooperation” and certain conditions which are described in more detail below.

The SEC and DOJ alleged that between 2006 and 2011, PTC China provided travel, gifts and entertainment to employees of Chinese state-owned entities in order to win and retain contracts. During this time period, PTC China provided personal travel to these government officials that was valued at nearly \$1.2 million and gifts and entertainment that was valued at more than \$250,000, generating approximately \$11.85 million in profits for the company.

PTC is a technology company that sells computer-aided drafting and project management software to customers in North America, Europe, and China. In China, U.S. authorities described a business model that included the engagement of a number of third parties—described as “business partners”—to provide lobbying or “influence services” and, in some instances, to also assist with information technology support services. These third parties often had long-standing relationships with government officials who worked for PTC China’s customers, and in some cases the government officials chose the specific business partners with whom they wished to collaborate. PTC China sales staff had wide discretion in setting the success fee arrangements with business partners, which ranged from between 15% and 30% of the contract price, and negotiated these fees on a deal-by-deal basis.

During contract negotiations with Chinese state-owned entities, government officials, sometimes in coordination with PTC China's business partners, would request that PTC China provide them with overseas travel that was ostensibly for training, but which in fact primarily involved tourist activities. According to PTC's policy, it was not supposed to pay for customers to travel to the United States for training. Nonetheless, PTC China, the officials, and PTC China's business partners would agree upon a travel budget for the contract and the Chinese government officials would then "gross up" the contract price to cover the travel costs. PTC China sales staff would itemize the travel costs in the contract documents for approval by senior PTC China personnel, but once the costs were approved, PTC China employees would remove the line items for travel before the contract documents were signed by PTC and the state-owned entities.

The travel arrangements typically included a one-day visit to PTC's facility, where PTC would demonstrate the company's products and services, followed by additional days of sightseeing that lacked any business purpose. Typical travel destinations in the United States included New York, Las Vegas, San Diego, Los Angeles, and Honolulu, and included guided tours, golf, and other leisure activities. The SEC noted that the officials who went on the trips were often the signatories of purchase agreements with PTC.

On one trip in September 2010, for example, a PTC China employee accompanied nine officials from three state-owned entities on a one-day trip to PTC's facility in Massachusetts, followed by sightseeing visits to New York, Los Angeles, Las Vegas, and Honolulu. An email discussing the visit noted that one of the attendees was not interested in overseas training, but instead wanted solely to engage in sightseeing activities. The DOJ noted that the Chinese customers whose employees went on the trip ultimately signed over \$3.5 million worth of agreements with PTC.

Expenses relating to travel for these officials were disguised and recorded as commissions and subcontracting expenses paid to the business partners, so that the costs of overseas travel did not raise suspicion with PTC's headquarters. The DOJ noted that when PTC discovered that a particular expense line item was being improperly used, PTC China began including the travel costs as part of its business partners' commissions in order to avoid detection by PTC. The SEC also noted that PTC China's sales staff tracked the travel payments made to the business partners on spreadsheets that were kept separate from PTC China's regularly maintained books and records in order to monitor the arrangements with the business partners and government officials.

Between 2009 and 2011, PTC China sales staff also provided at least \$250,000 in gifts and entertainment directly to Chinese government officials. The SEC alleged that the value of the gifts and entertainment ranged from between \$50 and \$600 and often included small electronics such as cell phones, iPods and GPS systems, as well as items such as gifts cards, wine and clothing. According to the SEC, PTC China provided these gifts in violation of PTC's policies which placed a limit of \$50 on gifts and entertainment provided to government officials, required PTC China sales staff to obtain pre-approval for expenses over \$500, and required PTC China sales staff to document the date, place, attendees and purpose of all business entertainment.

a. SEC Cease-and-Desist Order

The SEC alleged that PTC violated the anti-bribery, books and records, and internal accounting controls provisions of the FCPA. In addition to the conduct discussed above, the SEC noted numerous breakdowns of PTC's compliance program, including that compliance investigations of PTC China in 2006, 2008, and 2010, did not uncover or halt the improper payments to Chinese government officials. The SEC alleged that PTC also neglected to periodically assess the risks associated with PTC China, or to tailor its accounting controls to the risks presented by PTC China's particular circumstances. PTC China's Code of Ethics and Anti-Bribery policies were also vague and not based on the risks associated with Chinese operations, and PTC did not have independent compliance staff or an internal audit function that had authority to review and test internal accounting controls or intervene into management decisions.

In resolving these allegations through a settled cease and desist order, the SEC noted that PTC discovered the improper payments in 2011 and engaged independent counsel and an independent forensic consulting firm to undertake an investigation that was overseen by the Audit Committee of the Board of Directors. PTC then voluntarily self-reported the results of its internal investigation to the SEC and responded to information requests. The SEC noted, however, that PTC did not "uncover or disclose the full scope and extent of PTC China's FCPA issues until 2014." The SEC also acknowledged that PTC undertook significant remedial measures including terminating senior staff implicated in the violations, revising its pre-existing compliance program, updating and enhancing its financial accounting controls and compliance protocols and implementing additional specific enhancements in China.

b. DOJ Non-Prosecution Agreement

The DOJ agreed to refrain from pressing criminal charges against PTC China if the company complies with the terms of an NPA for a term of three years. The DOJ indicated that it agreed to resolve these allegations through an NPA given that, amongst other things, PTC China cooperated, at least partially, with the DOJ's investigation and PTC China undertook extensive remedial measures. Under the terms of the NPA, PTC China is required to self-report to the DOJ on the status of its compliance program remediation efforts. Within one year of signing the NPA, PTC China is required to submit a report detailing all remediation efforts, proposed improvements to the compliance program, and the scope of later reviews. PTC China must then conduct two annual follow-up reviews, tailored to any comments provided by the DOJ in response to the first report, and report on the results of these reviews to the Department.

24. PTC and Yu Kai Yuan

On February 16, 2016, the SEC announced that, for the first time, it had entered into a DPA with an individual to resolve FCPA allegations. The agency entered into a three-year DPA with Yu Kai Yuan, a former sales executive at PTC China to resolve allegations that Yuan caused PTC China to violate the books and records and internal accounting controls provisions of the FCPA. Yuan neither admitted nor denied the SEC's allegations, but agreed not to contest or contradict the factual statements contained in the Agreement in any future SEC enforcement action.

As discussed in more detail in our summary of the SEC and DOJ settlements involving PTC Inc. ("PTC") and PTC China, from 2006 until 2011, PTC China allegedly routinely provided gifts, entertainment, and personal travel for employees of Chinese state-owned entities in a corrupt effort to

obtain and retain business. PTC China provided the Chinese government officials with leisure travel throughout the United States that was valued at nearly \$1.2 million and often involved trips to locations such as New York, Hawaii, Las Vegas, and Washington, D.C. The true cost and nature of these trips was concealed by funding the travel through third party business partners who used their commissions and subcontracting fees to pay for the improper travel. In addition, the SEC claimed that PTC China provided the officials with more than \$250,000 in gifts and entertainment, often involving items such as iPods, GPS systems, gifts cards, wine and clothing. These gifts and entertainment were provided in many instances in violation of PTC's policies, which placed a limit of \$50 on gifts and entertainment that could be provided to government officials.

Although the DPA with Yuan recites many of the same allegations that were included in the SEC's cease-and-desist order with PTC, the agency does not make clear what role Yuan played in this misconduct. The agency merely notes that Yuan is a Chinese citizen who resides in Shanghai and that from 1996 until 2011 he was employed as a sales executive at PTC China.

This is the first time that the SEC has resolved FCPA allegations involving an individual through the use of a DPA. The SEC reiterated that "DPAs facilitate and reward cooperation in SEC investigations by foregoing an enforcement action against an individual who agrees to cooperate fully and truthfully throughout the period of deferred prosecution." The agency noted that it decided to resolve the allegations against Yuan through a DPA given Yuan's "significant cooperation" with the SEC's investigation.

The agency first used a DPA to resolve FCPA allegations against a company in May 2011 when it entered into a DPA with global steel manufacturer Tenaris SA, who had been accused of bribing government officials in Uzbekistan (and which is discussed below). The SEC's use of DPA to resolve these allegations was part of a larger effort, known as the Cooperation Initiative, which the SEC unveiled in early 2010 and ushered in a series of changes to SEC enforcement policy designed to encourage and reward cooperation. As part of the Cooperation Initiative, the SEC also introduced its first formal framework for evaluating cooperation by individuals. This framework is outlined in section 6.1.1 of the updated SEC enforcement manual and provides four factors that the SEC will consider in determining "whether, how much, and in what manner to credit cooperation by individuals." These factors are: 1) an assessment of the assistance provided by the cooperating individual in the investigation or related enforcement action, including whether the cooperation substantially aided the investigation, the timeliness of the cooperation, and the quality of the assistance, amongst other things; 2) the importance of the underlying matter, 3) the societal interests in ensuring that the cooperating individual is held accountable for his or her misconduct; and 4) the appropriateness of cooperation credit based upon the profile of the individual.

25. Qualcomm

On March 1, 2016, the SEC entered a cease-and-desist order in an internal administrative proceeding against Qualcomm Incorporated ("Qualcomm"), the world's largest mobile chipmaker, in a settlement for alleged violations of the FCPA's anti-bribery, books and records, and internal controls provisions with respect to the Company's operations in China from 2002 through 2012. Without admitting or denying the SEC's findings, Qualcomm agreed to pay a civil monetary penalty of \$7,500,000. The company also agreed to self-report to the SEC for two years on the status of its remediation and

implementation of compliance measures. During this two-year period, Qualcomm will conduct at least two reviews and submit at least two reports detailing its anti-corruption remediation efforts and compliance program proposals.

Michele Wein Layne, Director of the SEC's Los Angeles Regional Office, commented that, for over a decade, "Qualcomm went to extraordinary lengths to gain a business advantage with foreign officials deciding between Qualcomm's technology and its competitors."

Indeed, according to the SEC order, Qualcomm employed several means to influence the decisions of the relevant Chinese officials. First, Qualcomm allegedly provided frequent meals, gifts and entertainment to Chinese officials who were considering whether to adopt or retain Qualcomm-developed technology. According to the SEC order Qualcomm paid for gifts and hospitalities such as "airplane tickets for children of government officials, event tickets for spouses of foreign officials and luxury goods" as well as "golf outings" and "sightseeing [tours] for spouses and children of foreign officials", many of which had "no valid business purpose." Qualcomm apparently also offered luxurious hospitality packages for the 2008 Beijing Olympics worth almost \$100,000 (per couple) to at least fifteen foreign officials.

Second, and perhaps more importantly, this settlement is yet another illustration of alleged illicit hiring practices by Western companies in China pursuant to so-called "Sons and Daughters Programs" (as coined by the New York Times, when the newspaper initially revealed such practices by JPMorgan Chase). Indeed, Qualcomm allegedly offered full-time employment and paid internships to family members and referrals of foreign officials, designating some of these individuals as "must place" or "special" hires, despite the fact that they did not always meet the Company's hiring standard and had, in some cases, previously failed to be hired through the regular hiring process.

For example, in one case, where Qualcomm had initially decided to reject the son of an executive at a Chinese state-owned telecommunications operator because he did not have the requisite skills for the open position, the Human Resources director intervened, stating that the Company was "operating under a different paradigm here than a normal 'hire'/'no hire' decision tree." The company subsequently offered the son a \$75,000 research grant, an internship, followed by permanent employment at Qualcomm, and a business trip to China, notwithstanding concerns of other employees regarding his qualifications for these positions and assignments. The executive vice president and president of Qualcomm's Global Business Operations also personally provided the son with a \$70,000 loan to purchase a home.

When discussing Qualcomm's failure to devise and maintain adequate internal controls, the SEC in particular pointed to the fact that Qualcomm did not employ a chief compliance officer for its global operations, nor, specifically, for its Chinese operations, which generated almost half of the Company's revenues in 2012. While Qualcomm did not officially report the hiring of additional compliance staff, its press release following the SEC order indicates that the company had "taken additional steps to enhance its existing internal controls and procedures. For example, although like most organizations Qualcomm appreciates referrals of job candidates by those who know the candidates well, the Company now closely monitors to determine if a candidate has any relationship with an employee of a government agency or state-owned entity, and applies a stricter standard of scrutiny in an effort to avoid potential FCPA risks in the future."

The settlement with the SEC concluded what had been a long period of FCPA scrutiny regarding the Qualcomm's Chinese operations, not only by the SEC but also by the DOJ, during which the Company appeared to stand its ground. Indeed, pursuant to contemporaneous company filings, "on January 27, 2012, [Qualcomm] learned that the U.S. Attorney's Office for the Southern District of California/DOJ has begun a preliminary investigation regarding the Company's compliance with the Foreign Corrupt Practices Act (FCPA), a topic about which the SEC is also inquiring. The Company believes that it is in compliance with the requirements of the FCPA and will continue to cooperate with both agencies." In its March 2014 10Q, the Company disclosed that it had "received a Wells Notice from the SEC's Los Angeles Regional Office indicating that the staff has made a preliminary determination to recommend that the SEC file an enforcement action against the Company for violations of the anti-bribery, books and records and internal control provisions of the FCPA." According to the 10Q, Qualcomm, which had conducted an internal review led by the company's audit committee (with the assistance of outside counsel and forensic accountants) responded to the SEC on April 4, 2014 explaining "why the Company believes it has not violated the FCPA and [concluding that] therefore enforcement action is not warranted." While the DOJ notified Qualcomm on November 19, 2015 that it would not pursue the matter, the SEC persisted, eventually leading to the above-mentioned 7.5 million settlement.

26. Rolls-Royce

On January 17, 2017, prosecutors in the United States, the United Kingdom, and Brazil announced a global resolution with Rolls-Royce PLC ("Rolls-Royce"), a publicly traded multinational based in the United Kingdom with operations in industries ranging from civil and defense aerospace to oil and gas exploration and production. The global resolution settled charges by enforcement agencies from each of these countries that Rolls-Royce paid bribes to public officials around the world to influence the award of public contracts for more than a decade. The U.K. Serious Fraud Office ("SFO") also named Rolls-Royce's indirectly-owned, U.S.-based oil and gas subsidiary, Rolls-Royce Energy Systems Inc., ("RRESI"), as co-respondent.

Under the global settlement, Rolls-Royce and RRESI agreed to pay approximately \$800 million to resolve misconduct carried out between 1989 and 2013 across a number of countries, including Angola, Azerbaijan, Brazil, China, India, Indonesia, Iraq, Kazakhstan, Malaysia, Nigeria, Russia, and Thailand. The global penalty included approximately \$195.5 million to the U.S. DOJ, £497.3 million (\$604.8 million) to the U.K. SFO, and \$25.6 million to the Brazilian Ministério Público Federal ("MPF").

a. U.S. Deferred Prosecution Agreement

Rolls-Royce entered into a three-year DPA with the DOJ on December 20, 2016 relating to one count of conspiracy to violate the anti-bribery provisions of the FCPA. Under the terms of the DPA, Rolls-Royce agreed to a criminal penalty of \$195,496,880. Rolls-Royce's criminal penalty reflected a 25% discount on the lowest fine recommended by the U.S. Sentencing Guidelines. Rolls-Royce received this discount as a result of its extensive cooperation with the DOJ, termination of culpable-employees, termination of involved-third parties, enhancements to internal controls, and retention of an external compliance advisor to review and improve its compliance programs. Rolls-Royce also agreed to provide annual written compliance reports to the DOJ and the U.S. Attorney's Office for the Southern District of Ohio for the term of the DPA and to cooperate fully with the DOJ and U.S. Attorney in any and all matters

related to the conduct underlying the DPA. The DOJ also agreed to credit \$25.6 million to Rolls-Royce for the penalty it paid in Brazil to the MPF, bringing the total penalty payable to the U.S. to just under \$170 million.

Notably, the DOJ did not require Rolls-Royce to retain an independent compliance monitor despite the breadth, history, and repeated nature of the misconduct described in the charging documents. This is a break from the DOJ's recent trend of imposing an independent compliance monitor in cases where the misconduct was widespread and pervasive, as described by the DOJ in its settlements with Odebrecht, VimpelCom, Embraer, Och-Ziff, and others. While not explained by the DOJ, the decision not to require a compliance monitor may be related to Rolls-Royce's substantial pre-resolution enhancements to its compliance program, including the ongoing independent review of Rolls-Royce's compliance program being conducted by a U.K. compliance expert.

The conduct underlying Rolls-Royce's U.S. DPA involves approximately \$35 million in payments made by Rolls-Royce and RRESI between 2000 and 2013 to third parties in the oil and gas services industry with the knowledge that these payments would be used to bribe government officials in Angola, Azerbaijan, Brazil, Iraq, Kazakhstan, and Thailand. In return for these payments, government officials at several state-owned entities, including Asia Gas Pipeline, LLP in Kazakhstan, PTT Exploration and Production Public Company in Thailand, Petrobras in Brazil, the State Oil Company of the Azerbaijan Republic in Azerbaijan, SONANGOL in Angola, and South Oil Company in Iraq, provided Rolls-Royce and RRESI with confidential information and awarded contracts to Rolls-Royce, RRESI, and affiliated entities.

Rolls-Royce and RRESI used third parties, including intermediaries, consultants, agents, distributors, and commercial advisors, to facilitate and disguise its improper payments. In most cases, including the underlying conduct in Angola, Azerbaijan, Brazil, Kazakhstan, and Thailand, funds intended to be used as bribes were funneled to third parties as inflated commission payments. In other cases, additional funds were passed to third parties for services that were never performed, such as the engineering fees and related expenses paid to third parties in Thailand. Furthermore, Rolls-Royce and RRESI employees took steps to conceal the bribery schemes at work in these countries, including using personal email addresses, referring to officials by code names, and deleting emails from personal email accounts.

In Brazil, from 2003 to 2013, Rolls-Royce and RRESI caused more than \$9 million to be paid to intermediaries knowing that the intermediaries would pass a portion of these payments to a Petrobras official in order for RRESI to secure improper advantages and obtain business from Petrobras.

b. U.K. Deferred Prosecution Agreement

Rolls-Royce entered into a DPA with the U.K. SFO on January 17, 2017 in order to settle 12 total counts of conspiracy to corrupt, false accounting, and failure to prevent bribery brought under the U.K. Bribery Act. Rolls-Royce admitted to the conduct alleged by the SFO and agreed to pay a financial penalty, disgorgement of profits totaling £497,252,645 plus interest accrued, and the SFO's investigation costs of £13 million. Rolls-Royce also pledged to fully cooperate with the SFO in any additional investigation related to of the DPA's underlying conduct. The terms of the DPA apply through at least January 17, 2021, and may last through January 17, 2022, pending confirmation from the SFO that the

DPA has concluded. Rolls-Royce's DPA marks the SFO's third use of the DPA and represents by far the largest corruption investigation and settlement obtained by the SFO to date.

Under the U.K. DPA, the SFO did not require Rolls-Royce to retain a compliance monitor. Instead, the SFO pointed to the ongoing independent review of Rolls-Royce's compliance program being conducted by a compliance expert. Rolls-Royce retained the independent compliance expert starting in January 2013 to conduct an independent review of Rolls-Royce's anti-bribery and corruption compliance programs. The expert produced two interim reports dated June 10, 2013 and December 18, 2014, and was expected to produce a third report by March 31, 2017. The DPA required Rolls-Royce to provide a copy of the third report to the SFO within five days of its completion and to provide the SFO with a written plan to implement the third report's recommendations within approximately three months. The DPA provided Rolls-Royce with an additional 24 months to implement the recommendations from the report, at which point the SFO expects to review a final report.

The conduct underlying the DPA occurred in seven countries: China, India, Indonesia, Malaysia, Nigeria, Thailand, and Russia from 1989 to 2014. Over the course of three decades Rolls-Royce and RRESI repeatedly channeled millions in bribes to foreign officials through inflated commission payments made to third party advisors, consultants, and intermediaries. In exchange, officials from China Eastern Airlines, the Indian government, Garuda Indonesia, Nigerian National Petroleum Investment Management Services, Gazprom, and Thai Airways, among others, provided Rolls-Royce and RRESI with government contracts, confidential information, and preferential treatment. Rolls-Royce and RRESI also signed side letters, falsified contracts and invoices, and routed payments intended for a single beneficiary through several otherwise unrelated corporate entities in order to conceal the nature of its relationships with certain intermediaries, including in India where the use of third parties intermediaries in relation to defense contracts was prohibited. In Indonesia, Rolls-Royce even made payments to competitors' employees to ensure that the competitor submitted uncompetitive bids.

c. Brazilian Leniency Agreement

On January 17, 2017, Rolls-Royce agreed to a Leniency Agreement with the Brazilian MPF in which it agreed to pay a total of R\$81,183,700 (approximately \$25.6 million) for its role in a widespread conspiracy to bribe public officials between 2005 and 2008.

As discussed above, the conduct covered by the MPF Leniency Agreement overlaps with the conduct covered by the U.S. DPA. The DOJ credited the amount paid by Rolls-Royce to Brazilian authorities against its total U.S. penalties.

The Rolls-Royce agreement is the third major settlement agreement since October 2016 in which the Brazilian MPF has played a major role. The Rolls-Royce agreement, along with the Odebrecht/Braskem and Embraer settlements, is the result of Brazil's Operation Car Wash and demonstrates the degree to which the country and its enforcement authorities have embraced international cooperation as a tool against corruption.

27. SciClone Pharmaceuticals

On February 4, 2016, SciClone Pharmaceuticals, Inc. ("SciClone"), a California-based pharmaceutical company, agreed to pay more than \$12.8 million to settle Securities and Exchange

Commission (“SEC”) charges that it violated the anti-bribery, internal accounting controls and books and records provisions of the FCPA. The settlement consisted of \$9.426 million in profit disgorgement, prejudgment interest of \$900,000, and a \$2.5 million civil penalty; SciClone consented to the SEC’s cease-and-desist order without admitting or denying the SEC’s findings.

SciClone’s products are primarily sold in China. The company’s wholly owned, Cayman Islands-incorporated subsidiary, SciClone Pharmaceutical International, Ltd. (“SPIL”) and other subsidiaries are responsible for marketing and sales of SciClone products in China. The SEC found that, between 2007 and 2012, employees of SPIL and other SciClone subsidiaries offered money, excessive gifts, lavish vacations and travel, and other benefits and things of value to Chinese public officials, including healthcare professionals (“HCPs”) employed at state-owned or -controlled hospitals, for the purpose of increasing pharmaceutical sales. The SEC also found SciClone directed and oversaw the operations of SPIL and other subsidiaries, including by appointing their directors and officers, reviewing and approving annual budgets, and conducting direct oversight of the subsidiaries’ legal, audit and compliance functions. SciClone consolidated SPIL’s books and records and reported them in its financial statements.

a. Anti-Bribery Violations

The SEC alleged that, between 2007 and 2012, employees of SciClone subsidiaries provided “weekend trips, vacations, gifts, expensive meals, foreign language classes, and entertainment” to public official HCPs. Those who purchased the most SciClone products were designated as “VIP clients” and received special benefits, including vacations and trips to an annual golf- and beer-themed festival. Sales representatives reported information about these activities and their effects on sales to SPIL and SciClone officers; one report submitted by a sales representative explained how he dramatically increased sales to one HCP by paying for that HCP’s family vacations and regular family dinners.

SPIL also regularly hired Chinese travel companies to arrange transportation, accommodation, and meals for HCPs to attend ostensibly legitimate medical conferences and educational seminars, including in the United States, Japan, and on the resort island of Hainan, China. Many of these trips, however, did not actually include educational events, or the educational portion of the trip was dwarfed by the time spent on tourist or recreational activities. One seminar in Japan, for example, to which SPIL paid to send several Chinese HCPs, included half a day of education regarding a SciClone product and six days of sightseeing, including a visit to Mt. Fuji.

One particular incident in 2007 led to a limited internal investigation by SciClone. A regulatory affairs specialist hired by the company to facilitate licensing for a new medical device with the Chinese State Food and Drug Administration planned a trip for two foreign officials, who had oversight over licensing approvals, to attend an academic conference in Greece relevant to the applications of the new device. The officials, however, were unable to obtain travel visas in time to attend the conference; in lieu of the trip to Greece, the regulatory affairs specialist provided the officials with \$8,600 worth of lavish gifts. The specialist submitted expenses reimbursement requests for the gifts, one of which was approved by SPIL’s senior vice president. Upon learning of these gifts, SciClone fired the specialist and conducted an internal investigation related to the specialist’s activities; however, this review was ultimately of limited benefit to SciClone before the SEC because it did not extend to the company’s sales and marketing practices in China generally and did not result in any further remedial measures.

b. Books and Records and Internal Controls Violations

The SEC alleged that SciClone violated the books and records provision based on SPIL's practice of recording payments and gifts made to HCPs as sales, marketing, or promotional expenses. These inaccurate records were consolidated by SciClone and reported in its financial statements.

Additionally, the SEC alleged violations of the FCPA's internal controls provisions. It found that SciClone and its subsidiaries lacked internal controls to ensure that the "educational" conferences and seminars, to which it paid to send Chinese HCPs, had an appropriate business purpose and that the purported educational events actually occurred. A SciClone internal review also identified a high number of violations of the company's policy regarding the use of promotional accounts, including excessive gift or meal payments, doctored honoraria agreements, and the use of falsified or inaccurate fapiao. A fapiao is a paper receipt or an official invoice recognized by Chinese tax authorities as proof of a transaction. For example, a fapiao obtained by an employee for business expenditures, such as meals and travel expenses, is submitted by the company to claim a tax deduction for business expenses.

c. Remedial Efforts and Undertakings

Following the launch of the SEC's investigation in 2010, SciClone took a number of steps to investigate and remediate its conduct in China. As discussed above, the company conducted an internal review of employee promotion expenses, as well as a review of its internal policies and procedures regarding employee travel and promotional reimbursements, and third-party due diligence and payments. SciClone created internal audit and compliance departments, and hired a dedicated compliance officer for its China operations. Additionally, the company changed its practices towards third parties by substantially reducing the number of suppliers providing it with travel and event planning services, providing anti-corruption training to its travel and event planning vendors, and incorporating anti-corruption provisions into contracts with third parties.

As part of this settlement, SciClone agreed to submit periodic written reports to the SEC, as well as to report any new credible evidence it discovers, over a three-year period, of additional FCPA violations. The company agreed to submit to the SEC, within six months, an initial written report detailing its anti-corruption efforts to-date, as well as three follow-up reports during the three-year period.

A press release issued by the SEC acknowledged the assistance of the DOJ and FBI in conducting this investigation. In its own press release, SciClone stated that the DOJ had completed its own investigation and declined to pursue action against the company.

28. Teva Pharmaceuticals

On December 22, 2016, Teva Pharmaceuticals Industries, Inc. ("Teva") agreed to pay a combined \$519 million to the DOJ and SEC to resolve charges that it violated the FCPA by paying bribes to government officials in Russia, Ukraine and Mexico. Based in Israel, Teva is one of the largest generic drug manufacturers in the world. Teva's American Depository Receipts have been traded in U.S. markets since October 1987.

a. Russia

According to the DOJ and SEC, Teva and Teva's wholly-owned Russian subsidiary, Teva LLC ("Teva Russia"), agreed to make corrupt payments to a high-ranking Russian government official ("Russian Official") to influence the Russian government's purchase of Copaxone, a drug used to treat multiple sclerosis and one of the few non-generic products sold by Teva.

In mid-2009, the Russian government launched a new program which directed the government to purchase all pharmaceutical products primarily from domestic producers by 2020, with changes to the government's procurement auctions going into effect that year. Under the program, foreign pharmaceutical products repackaged in Russia would qualify for domestic preference.

In mid-2010, Teva Russia agreed with the Russian Official on a plan for the Russian Official, through a local wholesaling company he owned ("Russian Company"), to be Teva's repackager and distributor of Copaxone to the Russian government. Teva Russia, at the Russian Official's request, began giving the Russian Company discounts larger than discounts given to other Teva distributors in Russia. As a result of the significant discounts, from October 2010 to December 2012, the Russian Company earned a profit of approximately \$65 million from sales of Teva products.

When the proposed agreement was submitted through Teva's anti-corruption approval process, Teva Russia omitted critical information on the due diligence forms: that the Russian Official managed the Russian Company (although it was disclosed that the Russian Official's wife owned it), that the Russian Official was expected to help Teva Russia with sales to the Ministry of Health, and that the Russian Company's director was under investigation for corruption. The agreement passed Teva's anti-corruption approval process.

Despite withholding information in formal due diligence documentation, Teva Russia made clear to Teva executives that the Russian Official was involved in the Russian Company and that Teva Russia planned to use the Russian Official's connections at the Ministry of Health to benefit Copaxone's market share.

From October 2010 to December 2012, Teva earned approximately \$200 million from sales made to the Russian government with the assistance of the Russian Official.

In March 2013, the Russian Official resigned from his government position. By this time, Teva Russia was aware that the SEC had charged a U.S. company for FCPA violations partly due to payments the company made to the Russian Official and his companies. In August 2013, Teva Russia terminated its relationship with the Russian Company when the Russian Company refused to follow Teva's due diligence procedures.

b. Ukraine

According to the DOJ and SEC, from May 2002 to March 2011, Teva and its Ukrainian wholly-owned subsidiary ("Teva Ukraine") provided more than \$200,000 in cash, vacations, and other things of value to a Ukrainian government official ("Ukrainian Official") for his improper influence in the registration and promotion of various Teva drugs in Ukraine. These payments were improperly recorded as sales and marketing expenses and consultancy fees in Teva's books and records.

In Ukraine, drugs are required to be registered with the state, which tests and examines the drugs prior to their marketing and sale. The Ukrainian Official had senior positions within agencies under the Ukrainian Ministry of Health responsible for registering and approving drugs for marketing and sale. These senior positions gave the Ukrainian Official influence in approving drug registrations.

Between 2002 and 2011, Teva and Teva Ukraine engaged the Ukrainian Official as a third-party “registration consultant” through annual consultant agreements, agreeing to pay him monthly consulting fees. Teva also provided him with cash bonuses, travel expenses, and other things of value. Invoices indicated that the Ukrainian Official was paid for “registrations of Teva drugs.” Teva also paid for the Ukrainian Official’s numerous business class trips to Israel, including at least one trip where he was accompanied by his wife.

c. Mexico

The DOJ and SEC alleged that Teva’s Mexican subsidiaries (“Teva Mexico”) used a third-party distributor to pay bribes of between \$9,000 and \$30,000 to Mexican doctors and other healthcare providers to influence their Copaxone prescription decisions. In 2012, Teva Mexico paid bribes totaling almost \$160,000 to these doctors and healthcare providers. The SEC and DOJ estimated that Teva received benefits in the form of business valued at \$16,865,489.

Teva executives were aware of these payments as early as 2007. In 2007, Teva’s internal audit department received an anonymous letter stating that Teva Mexico was making payments to Mexican government officials with influence over regulatory approvals and drug purchase decisions in order to increase sales. Teva initiated and completed an internal investigation that resulted in the termination of 11 Teva Mexico employees connected with illicit payments. However, according to the SEC, Teva did not implement sufficient accounting controls to mitigate the corruption risks in Mexico and “sporadic misconduct” continued.

In early 2011, after Teva decreased Teva Mexico’s promotional budget for Copaxone, Teva Mexico began using a distributor to pay cash to doctors. Teva Mexico did not conduct due diligence on the distributor, as required by Teva’s anti-bribery policy, and did not require the distributor to sign an anti-corruption acknowledgment form.

The DOJ and SEC alleged that despite its awareness of corruption-related red flags and prior misconduct at Teva Mexico, Teva knowingly failed to implement an adequate system of internal controls and failed to enforce the controls it did have in place, including those requiring adequate due diligence on third parties.

The SEC noted that payments were authorized with little or no supporting documents. Although Teva’s 2006 Code of Conduct contained a section on FCPA requirements, Teva failed to publicize or enforce it. Even after learning of the violations in Mexico in 2007, Teva failed to implement FCPA policies in Latin America until 2009 and did not establish a global policy until 2010. Teva also did not establish a cohesive due diligence system and failed to vet some third-party vendors until 2013.

d. DPA, Plea Agreement, and SEC Complaint

Pursuant to a deferred prosecution agreement (DPA) with the DOJ, Teva admitted to one count of conspiracy to violate the anti-bribery provisions and one count of violating the internal controls provision of the FCPA. Teva Russia pleaded guilty to one count of conspiracy to violate the FCPA's anti-bribery provisions. As part of the DPA and guilty plea, Teva and Teva Russia agreed to pay a criminal penalty of \$283 million. Teva's total criminal penalty represents a 20% reduction off the bottom of the U.S. Sentencing Guidelines. The DOJ credited Teva for its cooperation with the investigation, remedial measures, and enhancements to its compliance programs.

Teva also settled a parallel investigation with the SEC related to charges that it violated the FCPA's anti-bribery, books and records, and internal controls provisions. In connection with its settlement with the SEC, Teva agreed to pay \$236 million in disgorgement and pre-judgment interest.

As part of the settlements with the DOJ and SEC, Teva also agreed to implement a corporate compliance program and retain an independent compliance monitor for a period of three years.

29. VimpelCom

On February 18, 2016, the DOJ, the SEC and the Public Prosecution Service of the Netherlands ("PPS") announced that they had reached a Global Foreign Bribery Resolution for \$795 million in penalties with VimpelCom Limited ("VimpelCom"), a multinational telecommunications company based in Amsterdam and publicly traded in the United States, and VimpelCom's wholly owned Uzbek subsidiary, Unitel LLC ("Unitel").

Between 2006 and 2012, VimpelCom paid over \$114 million in bribes to an Uzbek government official who was also a relative of Uzbekistan's President, Islam Karimov, and had substantial influence over the Uzbek Agency for Communications and Information ("UzACI"), the government agency with regulatory authority over the Uzbek telecommunications industry. According to widespread media reports, the recipient of the bribes was Karimov's daughter, Gulnara Karimova.

Under the terms of the global settlement, VimpelCom agreed to pay a \$460,326,398.40 fine and an additional \$335 million in disgorgement of unlawful profits, to be split equally between the United States and the Netherlands. VimpelCom also agreed to implement a compliance and ethics program designed to detect and prevent future FCPA and anti-corruption violations, review and enhance its internal controls, policies and procedures, retain an independent compliance monitor for a period of three years.

a. The Bribery Scheme

VimpelCom's bribery scheme involved a number of discrete stages of misconduct, starting with the process by which it initiated operations in Uzbekistan. Beginning in 2005, VimpelCom was looking to acquire an Uzbekistan subsidiary to expand its operations in the CIS region. VimpelCom decided to do so by purchasing two companies: Unitel and LLC Bakrie Uzbekistan Telecom ("Buztel").

At the time, Unitel was the second largest cellular service operator in the country with 300,000 subscribers, while Buztel had only 2,500 subscribers. From a commercial perspective, there was no clear

need to purchase Buztel in addition to Unitel, and a VimpelCom Finance Committee member even noted that funds used to purchase Buztel could be better spent on developing Unitel. However, members of VimpelCom management were aware that Karimova held an indirect interest in Buztel, considered that for “political reasons,” purchasing it would be “an entry ticket into the Uzbekistan market” and thought failing to do so could lead to negative consequences for Unitel operations in the country. Furthermore, Karimova appeared to have influence over the price VimpelCom would have to pay for Unitel.

VimpelCom’s board raised corruption concerns but approved acquisition of Buztel subject to FCPA analysis and approval from an international law firm. However, members of VimpelCom’s management aware of Buztel’s connection to Karimova concealed those facts from the law firm, and the FCPA analysis that resulted was favorable. In early 2006, VimpelCom purchased Buztel for approximately \$60 million and Unitel for approximately \$200 million, merging Buztel into Unitel shortly after the acquisitions.

The second stage of the bribery scheme involved VimpelCom entering into a partnership agreement in 2006 and 2007 with a Gibraltar-based company known as Takilant Ltd (“Takilant”), which was beneficially owned by Karimova through an associate. Under the partnership agreement, Takilant paid \$20 million for an indirect 7% stake in Unitel, with a guaranteed option to sell those shares back for at least \$57.5 million in 2009. As with the purchase of Buztel, VimpelCom’s board conditionally approved the agreement, pending a positive FCPA opinion from an external law firm, and specifically required that the “the identity of the Partner . . . [be] presented to and approved by the Finance Committee.” The legal analysis was again undermined by members of VimpelCom management, who failed to disclose that Takilant was controlled by Karimova, and Karimova’s true identity was likewise not disclosed at the Finance Committee meeting, where the issue was described as “extremely sensitive.” VimpelCom’s board approved the agreement in March 2007 and Takilant transferred \$20 million to VimpelCom in June 2007 for the 7% shares. Around September 2009, Takilant re-sold those shares for \$57.5 million.

The third stage of the bribery scheme involved VimpelCom funneling a \$25 million bribe to Karimova in November 2007 so Unitel could obtain licenses to operate a 3G cellular network in Uzbekistan. VimpelCom transferred \$25 million to Takilant, and in exchange, its wholly owned subsidiary repudiated the 3G licenses assigned to it and UzACI re-assigned them to Unitel. Documents prepared for a VimpelCom board meeting acknowledged that these licenses were not transferrable between private parties in Uzbekistan, but the board nevertheless unanimously authorized the \$25 million payment to Takilant. Members of VimpelCom management coordinated the transaction through the exchange of documents with government regulators, including a high-ranking official at UzACI, and the chief executive of Unitel’s primary competitors, who was an associate of Karimova acting on behalf of Takilant.

The fourth stage of the bribery scheme involved VimpelCom and its subsidiary engaging Takilant pursuant to phony consulting service contracts in 2008 and 2011 to provide Karimova with an additional \$32 million in bribes. In 2008, VimpelCom management crafted a sham consultancy agreement with Takilant covering nonexistent services in order to pay Karimova \$2 million she had demanded since the acquisition of Unitel in 2006. VimpelCom management structured the agreement to avoid scrutiny, created fake Takilant documentation connected to the agreement including Takilant’s invoice, and backdated other documentation to support the illusion that Takilant was providing legitimate services.

In 2011, VimpelCom executives again bribed Karimova by paying \$30 million to Takilant from a VimpelCom subsidiary, as compensation ostensibly for consulting services in connection with securing licenses for 4G frequencies. This was despite the fact that Unitel had no need for, or ability to utilize 4G frequencies in the near future. The proposed transaction prompted strong anti-corruption concerns within VimpelCom, including from a consultant serving as a VimpelCom senior executive at the time, who said they could "see no rationale" for paying Takilant to assist with obtaining the license while paying nothing to the Uzbek government, and said they would be unable to approve the transaction without "absolute transparency of our consultants' Gibraltar company [and] its ownership structure."

The FCPA analysis conducted by an external law firm was again fatally undermined. VimpelCom management continued to conceal Karimova's ownership of Takilant. No attorney ever contacted Karimova's associate, the ostensible owner of Takilant, and FCPA questionnaires were sent to intermediaries rather than directly to Takilant. In the face of the senior executive's concerns, VimpelCom in-house counsel claimed that additional due diligence was not warranted and that Takilant would be monitored to ensure real services were being provided. However, no one at VimpelCom made any such verification of Takilant's activities. Payment was made in September and October 2011 and on October 18, 2011 UzACI authorized Unitel to use 4G frequencies. Takilant provided activity reports pursuant to its consulting agreement that were almost wholly plagiarized from VimpelCom's own documents and internet sources, including Wikipedia entries.

In the fifth and final stage of the scheme, in 2011 and 2012, VimpelCom provided an additional \$20 million in bribes to Karimova through transactions with Uzbek "reseller" companies, which were generally used to circumvent Uzbek currency restrictions and in this case, further disguise the prohibited payments. Unitel contracted with local companies to pay inflated fees, denominated in Uzbek som (Uzbekistan's currency), for incidental or unnecessary services. Offshore affiliates of the Uzbek companies then sent wire payments denominated in U.S. dollars to Takilant's bank account in Switzerland. In 2011, VimpelCom routed a \$10 million payment to Takilant via the reseller mechanism, in return for which Takilant provided no legitimate services.

In 2012, VimpelCom executives executed transfer of an additional \$10 million to Takilant through reseller transactions through multiple Uzbek entities, despite receiving a whistleblower complaint from a Unitel employee about the transactions. The employee said they had discovered that a reseller company used by Unitel was located in a dilapidated, unmarked building, devoid of any technical staff, and, upon recommending that Unitel not use the reseller, they were pressured to resign. This complaint did not deter VimpelCom from making the 2012 payment. Additionally, VimpelCom and Unitel executives interfered with an internal audit of Unitel reseller transactions to further conceal the bribery scheme. In 2012 and 2013, VimpelCom executives conspired to pay an additional \$16 million in bribes to Karimova through reseller transactions in response to the threatened imposition of governmental and regulatory obstacles to Unitel's continued operations in Uzbekistan.

Finally, in addition to the over \$114 million in bribes paid to Karimova, VimpelCom made over \$500,000 in contributions to charities affiliated with Karimova. Unitel also paid \$38 million in connection with sponsorships and charitable contributions in Uzbekistan without properly verifying whether they were made for the benefit of government officials.

VimpelCom's bribery of Karimova continued without intervention for six years because of widespread, systematic compliance program and control failures. VimpelCom had no system in place for conducting true due diligence on third parties, and was free to enter into sham consulting agreements providing for inflated remuneration, payable to bank accounts in jurisdictions with no connection to the consultant or services provided. It had no policy or structure to regulate and oversee single-source contract decisions like the above-mentioned reseller transactions, which were exploited by VimpelCom executives to pay bribes. VimpelCom failed to operate effective internal audit processes and failed to monitor and control its transactions for conflicts of interest.

VimpelCom's internal control failures were possible due to its lack of adequate compliance structures and personnel. At the time of its purchase of Unitel and Buztel, VimpelCom had no Chief Compliance Officer. The individual later selected to serve this role was underqualified and given drastically inadequate resources. VimpelCom conducted essentially no internal anticorruption program, and its legal department provided no substantive review of its transactions for FCPA compliance and relied on analysis by external law firms. This created an environment where VimpelCom executives could easily manipulate the process to conceal their bribery.

b. Terms of the Global Resolution

VimpelCom admitted, pursuant to a deferred prosecution agreement, to conspiring to violate the FCPA's anti-bribery and books and records provisions and violating the FCPA's internal controls provision, and agreed to pay a \$460,326,398.40 fine, split equally between the United States and the Netherlands. \$40 million of the portion of the fine paid to the United States was designated forfeiture of proceeds from transactions in violation of the FCPA. Unitel pleaded guilty to conspiracy to violate the anti-bribery provisions of the FCPA but was not separately fined in light of VimpelCom's fine and the interrelated nature of the conduct at issue.

VimpelCom's fine was 45% below the low end of the applicable United States Sentencing Guide fine range, reflective of: i) a "full cooperation and remediation credit" of 25% for, inter alia, providing the DOJ with evidence uncovered in its internal investigation and conducting additional investigative efforts; and ii) a 20% reduction for promptly acknowledging the misconduct of its personnel and exhibiting willingness to resolve criminal liability on an expedited basis after being notified it was subject to criminal investigation. The DOJ also took into consideration VimpelCom's extensive remediation efforts, including a complete overhaul of its compliance program, its agreement to be subject to an independent compliance monitor selected by the DOJ for three years, its continued cooperation with further investigations related to the company, and the absence of any prior criminal history.

The DOJ noted that VimpelCom's fine would have been reduced further and/or would have had fewer remedial measures imposed upon it had it voluntarily self-reported the misconduct it had discovered through its original internal investigation.

The SEC separately reached a settlement with VimpelCom, entered as a final judgment, on February 22, 2016, for disgorgement of \$375 million in profits derived from VimpelCom's unlawful conduct – less a credit for \$40 million related to the forfeiture portion of the fine paid pursuant to the VimpelCom DPA – to be paid equally to the United States and the Netherlands.

Finally, the DOJ also filed a civil complaint in the Southern District of New York seeking forfeiture of more than \$550 million in Swiss bank accounts constituting alleged corrupt payments made by VimpelCom and other telecommunications companies. This follows a prior complaint filed January 11, 2016 that sought forfeiture of \$300 million in corrupt payments in bank accounts in Belgium, Luxembourg and Ireland.

In announcing the global resolution, the DOJ and the SEC acknowledged the significant cooperation and assistance it had received from – in addition to the Dutch PPS – the Swedish Prosecution Authority, the Office of the Attorney General in Switzerland, the Corruption Prevention and Combating Bureau in Latvia, and the National Authority for Investigation and Prosecution of Economic and Environmental Crime in Norway. The DOJ expressed its gratitude for the support provided by law enforcement in Belgium, France, Ireland, Luxembourg and the United Kingdom. The SEC similarly thanked financial regulators in the British Virgin Islands, the Cayman Islands, Bermuda, Ireland, Estonia, Spain, Latvia, UAE, the Marshall Islands, and Gibraltar for their assistance.

30. Jun Ping Zhang

On September 13, 2016, U.S. citizen and resident Jun Ping Zhang (“Ping”) settled claims with the SEC related to violations of the FCPA’s anti-bribery, books and records, and internal controls provisions. Ping is the former Chairman and CEO of Hunan CareFx Information Technology, LLC (“CareFx China”) and former Vice President of Technology at CareFx China’s ultimate parent company Harris Corporation (“Harris”). Without admitting or denying the allegations, Ping agreed to pay a civil penalty of \$46,000 to resolve claims that he violated, and caused others to violate, the FCPA’s anti-bribery, books and records, and internal controls provisions related to the business practices of CareFx China. The DOJ and SEC declined to pursue charges against Harris for alleged books and records violations caused by Ping.

a. SEC Allegations

According to the SEC’s cease-and-desist order, from April 2011 to April 2012, CareFx China distributed up to \$1 million in improper gifts, entertainment, and payments to Chinese government officials affiliated with state-owned hospitals and local Chinese health departments, which comprised CareFx China’s customer base. In turn, those officials awarded over \$9.6 million in contracts to CareFx China.

The SEC alleged that Ping was aware of and endorsed the scheme, even if he did not personally authorize every bribe. For example, the SEC pointed to an instance in approximately April 2011 when a CareFx China sales manager sent an email requesting approval to spend RMB20,000-RMB30,000 (\$3,000-\$4,600) on electronics and vacation expenses for various high-level officials at Wuhan University Zhongnan Hospital (“Zhongnan Hospital”). The sales manager urged that such funds were necessary, stating, “If we don’t do this, sooner or later some other company will. This is how the business environment is in China.” Ping was copied on the e-mail, to which he replied, “You are doing a great job. This is very exciting. Thanks.” The final number submitted for reimbursement was increased to RMB36,100 (\$5,300) to include additional vacation travel and entertainment costs for Zhongnan Hospital officials. Later that year, that hospital awarded roughly \$165,000 in contracts to CareFx China.

The SEC further alleged that Ping and CareFx China used several tactics to conceal the scheme from Harris, CareFx China’s ultimate parent company. First, Ping warned employees to avoid giving gifts

that were too valuable. Second, sales managers submitted—and Ping approved—receipts with falsified descriptions for reimbursement. The gifts and entertainment for Zhongnan Hospital officials were submitted as “business meeting receipts,” for example. Third, CareFx China also falsified descriptions when it recorded improper expenses in its books and records, using narratives such as “office expenses” and “conference expenses” to account for money spent on public officials. According to the SEC, these false financial records were an attempt by Ping to conceal CareFx China’s bribery scheme from Harris and circumvent Harris’s internal control system.

b. Acquisition, Internal Investigation, and Closure of CareFx China

Harris is a Delaware corporation headquartered in Melbourne, Florida. Harris provides services in communication and information technology to public and private sector customers worldwide. Harris acquired CareFx China’s parent company, Arizona-based CareFx Corporation (“CareFx”), in April 2011. Ping continued to serve as CareFx China’s Chairman and CEO after the acquisition.

Following internal allegations by staff that CareFx China had made improper payments to Chinese officials, Harris launched an internal investigation of its new subsidiary. In the course of the investigation, Harris removed Ping from his positions as CareFx China’s Chairman and CEO in April 2012, and terminated Ping’s other services at Harris in July 2012. In its August 27, 2012 Form 10-K filed with the SEC, Harris disclosed that CareFx China had potentially violated the FCPA, also noting that Harris had shared its investigation findings with the SEC and DOJ.

The SEC order indicated that Harris had incorporated CareFx’s books and records into its financial statements before dissolving CareFx Corporation as a separate business entity in December 2011. Harris sold all the “outward facing operations” of CareFx China in September 2012, after the conclusion of its internal investigation. Harris terminated all CareFx China employees on June 12, 2015 and has had no active business operations based in China since that time.

c. Resolution

The SEC found that Ping’s actions caused Harris to violate the FCPA’s books and records provisions. However, both the DOJ and SEC declined to prosecute Harris. According to Harris’s January 2016 quarterly report, the DOJ informed Harris in 2015 that it would not face any enforcement action from the DOJ. The DOJ reportedly based its decision on Harris’s due diligence, voluntary disclosure, remediation, and cooperation.

The SEC announced its declination on September 12, 2016, in tandem with its announcement of the settlement with Ping. The press release emphasized Harris’s “immediate and significant steps” to fold CareFx China into its compliance systems, noting that Harris discovered the irregularities only five months after acquiring CareFx China. It also credited Harris’s self-reporting, remediation, and cooperation.

Although Harris received the DOJ’s declination before the implementation of the DOJ Pilot Program, the weight the DOJ granted to Harris’s remediation, voluntary disclosure, and cooperation appears to mirror the factors considered under the Program. And, while the SEC does not have a Pilot Program analogue, its decision indicates that it attaches similar importance to those factors. The choice by the DOJ and SEC not to charge Harris emphasizes the importance and wisdom of thorough pre- and post-acquisition due diligence.

The SEC order imposed a \$46,000 penalty against Ping, but implemented no additional restrictions beyond a general prohibition against further violating, or causing others to violate, the FCPA.

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. *United States Developments and Regulatory Guidance*

1. DOJ Compliance Guidelines

In February 2017, the DOJ Fraud Section issued its Evaluation of Corporate Compliance Programs (“Compliance Guidelines”) which provides further insight into the factors that the DOJ will consider in assessing the effectiveness of a corporate compliance program as prosecutors conduct investigations, determine whether to bring charges, and negotiate plea or other agreements. Though the Compliance Guidelines do not materially change companies’ obligations, they do provide helpful signposts for internal and external counsel and compliance officers.

The Compliance Guidelines cover eleven topics that align in large part with sections included in the United States Attorney Manual, United States Sentencing Guidelines, the DOJ’s Resource Guide to the FCPA (“FCPA Guide”), and the Organization for Economic Cooperation and Development Anti-Corruption Ethics and Compliance Handbook for Business. Each topic includes guidance on relevant subtopics and questions that the DOJ is likely to use in assessing a company’s corporate compliance program. The eleven subjects covered by the Compliance Guidelines are:

- Analysis and Remediation of Underlying Misconduct, which includes a root cause analysis, consideration of whether there were prior opportunities to detect the misconduct and, if so, why such opportunities were missed, and an assessment of the company’s remediation efforts;
- Senior and Middle Management, which focuses on senior leaders and other stakeholders’ conduct, messaging, and demonstrated commitment to compliance, as well as compliance oversight by the board of directors;
- Autonomy and Resources, including questions designed to assess whether the compliance function has sufficient autonomy, funding, resources, and experience, to fulfill its role;
- Policies and Procedures, which addresses the design—such as whether there were policies in place prohibiting the misconduct in question—and communication and operational integration of compliance policies and procedures;
- Risk Assessment, which focuses on the methodology used to assess risks and the nature of the response to such identified risks;
- Training and Communications, including the form, content, and efficacy of training to address the most significant risks faced by the trainees, as well as the availability of guidance regarding compliance policies;

- Confidential Reporting and Investigation, which addresses the company's reporting mechanism, scoping of any subsequent investigation, and response to identified root causes, system vulnerabilities and accountability lapses;
- Incentives and Disciplinary Measures, focusing on whether and how the company held employees and managers responsible for the misconduct in question, and whether the company has incentivized compliance and ethical behavior;
- Continuous Improvement, Periodic Testing and Review, which includes questions on what types of audits would have identified issues relevant to the misconduct, whether the company has undertaken these types of audits and control tested its compliance program, and whether the company regulates its compliance policies sufficiently frequently to respond to identified risks;
- Third Party Management, which focuses on whether the company's processes for engaging third parties is responsive to identified risks and whether the company has in place sufficient controls and oversight of third parties; and
- Mergers and Acquisitions, which addresses the company's M&A due diligence process and whether and how thoroughly the compliance function and the compliance policies and procedures have been integrated into the M&A process.

In April 2017, Attorney General Jeff Sessions confirmed that the Trump Administration's Department of Justice would continue to take into account the quality of a company's compliance programs, among other factors, in charging decisions.

The DOJ's first compliance counsel, Hui Chen, who was responsible for, among other things, assessing companies' corporate compliance programs resigned abruptly in July 2017. The position of compliance counsel at DOJ does not appear to have been filled.

2. Rulings on the Statute of Limitations in Civil Penalty Actions

Recent rulings provide some clarity and additional limitations on when the SEC may file civil complaints to enforce the FCPA and other securities laws under 28 U.S.C. § 2462. 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.

Over the past several years, the Supreme Court and lower federal courts have issued rulings interpreting § 2462, each time seemingly further restricting the SEC's enforcement reach over historical violations.

i. Limitations Period Applies to Certain Declaratory Relief

On February 27, 2013, the Supreme Court held in *Gabelli v. SEC* that the statute of limitations clock for civil penalties begins when a violation of securities law is completed, not when the violation is

discovered. In May 2016, in *SEC v. Graham*, the 11th Circuit held that § 2462 applies to certain declaratory relief as well as 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. Limitations Period Applies to Disgorgement

In June 2017, in *Kokesh v. SEC*, the U.S. Supreme Court ruled that the statute of limitations imposed by § 2462 applies not only to civil penalties but also 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.

3. SEC Whistleblower Program

The SEC whistleblower program was established in 2011 pursuant to Section 922 of the Dodd-Frank Act (“Act”). The program is administered by the SEC’s Office of the Whistleblower, an office within the Division of Enforcement. The program allows the SEC to pay awards to whistleblowers who voluntarily provide original information that leads to the successful SEC enforcement actions that result in monetary sanctions in excess of \$1 million. Under the Act, the SEC may award between 10% and 30% of monetary sanctions collected. On May 25, 2011, the SEC adopted Rule 21F that established the program, and it became effective in August 12, 2011.

From its inception through July 2017, the Commission has awarded over \$158 million to 46 whistleblowers, including a \$30 million award in September 2014 and a \$17 million award in June 2016. The SEC has also received an increasing number of tips from potential whistleblowers for violations relating to offering fraud, manipulation, trading and pricing, market events, and the FCPA. For instance, whistleblower tips have grown from 3,238 in the 2013 fiscal year to 4,218 in 2016. Submissions are also geographically dispersed. In FY 2016, the Commission received submissions from individuals in 67 foreign countries, with the highest number from Canada (68), the United Kingdom (63), Australia (53), China (35), Mexico (29), and India (20). The remaining sources of FY 2016 whistleblower tips are a diverse cross-section of the world’s nations, such as Brazil (7), Ireland (14), Columbia (2), Israel (8), South Africa (8), Thailand (1), and Taiwan (13).

While the majority of tips relate to non-FCPA topics, the SEC continues to receive a significant and increasing number of tips relating to FCPA violations, including 115 tips in FY 2012 and 238 tips in FY 2016. Because none of these tips have resulted in a qualifying settlement thus far, the program has not yet issued its first FCPA-related award.

Since the enactment of the Dodd-Frank Act, the SEC has brought enforcement actions to emphasize that companies cannot stifle whistleblowers through confidentiality agreements. Courts have also wrestled with the appropriate scope of protections for employee whistleblowers. Recent cases indicate that there may be some tension between the SEC and courts regarding the interpretation of Dodd-Frank whistleblower protections, particularly whether whistleblowers must report to the SEC to qualify for Dodd-Frank protections against retaliation.

a. Companies Cannot Stifle Whistleblowers through Confidentiality Agreements

On April 1, 2015, the SEC announced its first enforcement action for violations of whistleblower protections under Rule 21F-17, which provides that “[n]o person may take any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement . . . with respect to such communications.”

Under the terms of a cease and desist order, KBR, Inc. (“KBR”), a Delaware corporation listed on the NYSE, agreed to pay a civil penalty of \$130,000 and make specific remedial actions for stifling

whistleblowers through confidentiality agreements. According to the SEC, KBR's compliance program used a form confidentiality statement that prohibited employees who were participating in internal investigation interviews from disclosing details of the interview to third parties without the prior authorization of KBR's legal department. Penalties for violation included disciplinary actions, up to termination. The Commission found that these confidentiality obligations undermined the incentive to report and therefore violated Rule 21F. In its Press Release regarding the KBR settlement, the Commission noted that "KBR changed its agreements to make clear that its current and former employees will not have to fear termination or retribution or seek approval from company lawyers before contacting" the SEC.

Two similar actions were announced in August 2016. On August 10, 2016, the SEC announced a settlement with BlueLinx Holdings Inc. ("BlueLinx"), a Delaware corporation trading on the NYSE. BlueLinx agreed to pay a civil penalty of \$265,000 for adopting language in severance agreements that, in violation of Rule 21F, prohibited sharing confidential information "unless compelled to do so by law or legal process." The agreements further required employees to provide written notice or obtain written consent from the company's legal department prior to providing information pursuant to such legal process. As with the KBR case, the confidentiality provisions did not exempt employees from voluntarily disclosing possible violations to the SEC or other enforcement agencies. The SEC found that BlueLinx violated legal protections by impeding participation in the whistleblower program and by "forc[ing] employees to choose between identifying themselves to the company as whistleblowers or potentially losing their severance pay and benefits." In addition to the civil penalty, the company modified its agreements to allow reporting of securities violations to federal agencies without approval, and to contact former signatories of these agreements and notify them of changes.

On August 16, 2016, the SEC announced that Health Net, Inc. ("Health Net"), a California-based health insurance provider, agreed to pay \$340,000 for violations of Rule 21F in relation to employee severance agreements that included a clause for waiver and release of potential claims. Following the effective date of the regulations, the company amended the clause to allow participation in government investigations but also prohibited the filing or acceptance of SEC whistleblower awards. In June 2013, the company further amended its agreements to exclude the express prohibition against applying for SEC whistleblower awards but included a broader waiver of rights to "any individual monetary recovery . . . in any proceeding brought based on any communication by Employee to any federal, state, or local government agency or department." While the SEC noted that it was unaware of cases where former employees were restrained by the agreements or where Health Net took action to enforce the agreements, it found that Health Net's removal of "critically important financial incentives" for direct SEC communications violated the rule. In addition to the penalty, Health Net agreed to contact its former employees that had signed the agreements and inform them of these changes.

b. Circuit Split Regarding Whether Whistleblowers Must Report to the SEC to Qualify for Dodd-Frank Retaliation Protections

On August 4, 2015, the SEC released interpretative guidance on anti-retaliation protections provided under the whistleblower provisions as implemented by the SEC's own Exchange Act Rules. The guidance sought to clarify who qualifies as a whistleblower under the Dodd-Frank Act's anti-retaliation provisions, and to respond to the Fifth Circuit's decision in *Asadi v. GE Energy*. The Fifth Circuit's 2013 *Asadi* decision limited retaliation protections to employees who report securities law violations to the SEC

and excluded those who reported only within an organization's internal structure. The SEC's 2015 interpretative guidance took a different position, expounding on arguments made in the SEC's *Asadi* amicus brief. The SEC's 2015 Guidance interprets Section 21F's retaliation protections to apply to whistleblowers who suffer adverse consequences from reporting internally regardless of whether reports were made to the SEC and whether the whistleblower may qualify for whistleblower awards (which require reporting to the SEC). The Commission described this interpretation as reasonable, stating:

Specifically, by providing employment retaliation protections for individuals who report internally first to a supervisor, compliance official, or other person working for the company that has authority to investigate, discover, or terminate misconduct, our interpretive rule avoids a two-tiered structure of employment retaliation protection that might discourage some individuals from first reporting internally in appropriate circumstances and, thus, jeopardize the investor-protection and law-enforcement benefits that can result from internal reporting.

There appears to be growing support for this position. On September 10, 2015, the Second Circuit issued a 2-1 decision in *Berman v. Neo@Ogilvy LLC*, reversing and remanding a decision by the District Court for the Southern District of New York that dismissed a plaintiff's claim for retaliation protections on the grounds that reports were only made internally. While acknowledging that its decision created a circuit split between the Second and Fifth Circuits, the Court observed that "a far larger number of district courts have deemed the statute ambiguous and deferred to the SEC's Rule." The majority opinion concluded that the provisions of the Dodd-Frank Act "create a sufficient ambiguity to warrant . . . deference to the SEC's interpretive rule." On March 8, 2017, the Ninth Circuit ruled in *Somers v. Digital Realty Trust Inc.* that an employee who reportedly alleged wrongdoing purely internally and not to the SEC was entitled to the whistleblower protections of the Dodd-Frank Act, adopting the SEC and Second Circuit's positions. In doing so, the Ninth Circuit noted that the narrower Fifth Circuit reading of the rule would narrow the whistleblower protections "to the point of absurdity."

The Supreme Court appears poised to address this growing circuit split. On June 26, 2017, the Supreme Court granted *certiorari* for *Somers v. Digital Realty Trust Inc.* and will hear oral arguments on November 28, 2017. On October 17, 2017 the Solicitor General filed a motion for leave to participate in oral arguments and *amicus curiae* brief in support of the SEC's interpretation.

4. Kleptocracy Asset Recovery Initiative

In July 2010, then-Attorney General Eric Holder announced the creation of the Kleptocracy Asset Recovery Initiative ("Kleptocracy Initiative"), which aims to combat large-scale foreign official corruption by targeting the recipients of corrupt funds in actions to recover money and other assets obtained by foreign officials through corrupt means, and, when possible, use the funds to benefit the victims of the corruption. While seizing assets purchased from corrupt foreign proceeds is not new to the DOJ, the Kleptocracy Initiative was launched to increase focus and cooperation in the DOJ's fight against public corruption and to keep the U.S. from becoming a safe haven for assets pilfered by foreign kleptocrats. Since its creation, the Kleptocracy Initiative has been spearheaded by prosecutors in the Asset Forfeiture and Money Laundering Section ("AFMLS") of the DOJ Criminal Division. These prosecutors work in partnership with U.S. Attorneys' Offices and other federal law enforcement agencies, including the Federal Bureau of

Investigation (“FBI”), the Department of Homeland Security, and the International Revenue Services (“IRS”) (all of which have specialized teams dedicated to international corruption cases). Additionally, the Kleptocracy Initiative seeks to foster increased cooperation and support from international authorities and communities in its asset recovery activities and provide assistance to foreign countries seeking to recover assets located in the U.S.

The main weapon for prosecutors in the AFMLS, and other offices involved in the Kleptocracy Initiative, is the U.S. government’s “confiscation authority.” The confiscation authority allows the U.S. to initiate forfeiture actions against any property, real or personal, within U.S. jurisdiction that constitutes, is derived from, or is traceable to various domestic and foreign offenses, including the misappropriation of public funds by or for the benefit of a public official. Since its inception, the Kleptocracy Initiative has used this confiscation authority, in addition to other asset recovery tools such as mutual legal assistance requests, to recover funds around the world traceable to corrupt schemes perpetrated by foreign officials from countries such as Nigeria, Equatorial Guinea, Ukraine, Uzbekistan, Kazakhstan, South Korea, Taiwan, and most recently Malaysia.

Two high-profile Kleptocracy Initiative actions are discussed below in detail.

a. 1MDB

1Malaysia Development Berhad (“1MDB”), a wholly-owned Malaysian government fund, was created to strategically invest and develop projects for the economic benefit of Malaysia and its people. Instead, according to the DOJ, from 2009 to at least 2014, 1MDB’s funds were systemically siphoned by public officials and their co-conspirators, mainly over four different phases: (i) the “Good Star” phase (2009-2011); (ii) the “Aabar-BVI” phase (2012); (iii) the “Tanore” phase (2013); and (iv) the “Options Buyback” phase (2014).

The “Good Star” Phase: According to the DOJ, 1MDB officials and their co-conspirators diverted funds from 1MDB’s bank account to a Swiss bank account held in the name of Good Star Limited (“Good Star”). The Good Star account was beneficially owned by Jho Low (“Low”), a well-connected Malaysian who has no formal position within 1MDB but was involved in its creation. The DOJ has alleged that between 2009 and 2011, officials at 1MDB, under the pretense of investing in a joint venture between 1MDB and PetroSaudi, a private Saudi oil extraction company, provided false information to banks about the ownership of the Good Star account and fraudulently wired more than \$1 billion of funds from 1MDB to the Good Star account. From these funds, the conspirators are accused of sending more than \$400 million into the United States to be used by Low and others to cover gambling debts at Las Vegas casinos, rent luxury yachts, and purchase luxury real estate and a \$35 million Bombardier jet.

The Aabar-BVI Phase: In 2012, two separate bond offerings were held to raise funds for 1MDB to invest, for the benefit of the Malaysian government, in certain energy assets. The bond issuances were jointly guaranteed by 1MDB and the International Petroleum Investment Company (“IPIC”), an investment fund wholly-owned by the Abu Dhabi government. The DOJ has alleged that almost immediately after those offerings, certain officials and their associates wired \$1.37 billion, approximately 40% of the funds raised, out of 1MDB’s account to a Swiss bank account held by a shell company incorporated in the British Virgin Islands (“BVI”). The BVI shell company was named Aabar Investments PJS Limited (Aabar-BVI), which was purposefully similar to Aabar Investments PJS, a legitimate subsidiary of IPIC. In a

March 2014 financial statement, 1MDB is alleged to have fraudulently recorded the payments to Aabar-BVI, the BVI shell company, as an asset, describing it as a “refundable deposit” held aside as collateral for the guarantee. However, the DOJ alleged that in reality the funds were transferred in a series of transactions to other shell companies and bank accounts to be used for the personal benefit of corrupt officials and their associates. For example, the DOJ has alleged that \$238 million ended up in a Singaporean bank account held by Red Granite Capital, an entity owned by Riza Aziz, the stepson of a senior 1MDB official (whom the press has identified as Malaysian Prime Minister Najib Razak). According to the DOJ complaints, Aziz used the money to buy U.S. luxury real estate and to fund Red Granite Pictures, a California-based motion picture company. Red Granite Pictures ultimately used more than \$100 million of the funds to finance *The Wolf of Wall Street*, a 2013 Academy-Award-nominated movie.

The “Tanore” Phase: In 2013, 1MDB raised \$3 billion in a bond offering to promote growth in Malaysia and Abu Dhabi. The DOJ has alleged that 1MDB officials diverted \$1.26 billion from this bond offering to a Singaporean bank account held in the name of Tanore Finance Corporation (“Tanore”), an entity beneficially owned by Tan Kim Loong (“Tan”), an associate of Jho Low. According to the DOJ, shortly after the bond offerings closed, \$681 million was transferred from the Tanore bank account to other accounts owned or controlled by Tan, Low, and their associates. The corrupt proceeds were allegedly used by Tan and Low to purchase \$137 million in artwork, including a \$35 million work by Claude Monet; an interest (purchased for \$106 million) in the world’s third largest music publishing company, EMI Music Publishing; and an interest in the Park Lane Hotel in New York City.

The “Options Buyback” Phase: In connection with IPIC’s guarantee of bonds issued by 1MDB in 2012 (described above), Aabar Investments PJS, the legitimate subsidiary of IPIC, had been awarded options to acquire a stake in certain energy assets held by 1MDB. In 2014, 1MDB decided to buy back these options from Aabar Investments PJS, and approached Deutsche Bank about obtaining loans to finance this purchase. In May 2014, Deutsche Bank made \$250 million available to 1MDB, most of which was immediately transferred to the Swiss bank account held by Aabar-BVI, a BVI shell company (described above) owned by 1MDB officials and their associates but allegedly meant to appear to be affiliated with IPIC. In September 2014, Deutsche Bank extended an additional \$975 million loan to 1MDB for the agreed purpose of refinancing the earlier loan and completing the option buyback. The majority of these funds were quickly transferred to a Singapore bank account held by a recently incorporated, Seychelles-based company also named Aabar Investments PJS Limited (Aabar-Seychelles). Like Aabar-BVI, Aabar-Seychelles was owned by 1MDB officials and their associates but allegedly meant to appear to be affiliated with IPIC. In order to secure these loans, the DOJ alleges that 1MDB made fraudulent disclosures about its assets and the terms of the options buyback agreement. Additionally, a Malaysian official (“Malaysian Official”) (identified in the press as Malaysian Prime Minister Najib Razak) guaranteed to Deutsche Bank that the Government of Malaysia would ensure that the \$975 million loan would be repaid. In total, approximately \$850 million was transferred to Aabar-BVI and Aabar-Seychelles. The DOJ alleges that these funds were diverted to the personal accounts of public officials and their associates, used by Low to purchase a 300-foot yacht, and cycled through various accounts to make it appear that 1MDB still retained billions in assets which had actually been spent or diverted to officials’ personal accounts.

On July 20, 2016, the DOJ, FBI, and IRS held a joint press conference to announce the largest collective civil forfeiture actions ever under the Kleptocracy Initiative, with complaints aimed at recovering more than \$1 billion in assets tied to the alleged public corruption and global money laundering conspiracy at 1MDB.

The July 2016 actions brought by the DOJ sought civil forfeiture of more than \$1 billion worth of assets traceable to funds that the DOJ identified as having been laundered through U.S. financial institutions, and included forfeiture complaints directed against assets such as a Bombardier aircraft; EMI Music; several luxury real estate properties located in New York, California, and London; artwork by Monet and Van Gogh; and future interests (including copyright and intellectual property rights, as well as rights to profits, royalties, and distribution proceeds) in the film *The Wolf of Wall Street*.

In June 2017, the DOJ filed additional civil forfeiture actions seeking to recover approximately \$640 million in further assets tied to what it described as an “international conspiracy to launder funds misappropriated from [1MDB].” The assets identified in these actions include The Equanimity, a 300-foot luxury yacht purchased for more than \$250 million; stock in U.S. companies; and rights and interests in the films *Dumb and Dumber To* and *Daddy’s Home*. These actions also sought to recover additional jewelry and artwork valued in the tens of millions of dollars, including over \$27 million of jewelry purchased for a woman identified in the press as the wife of the Malaysian Prime Minister; approximately \$8 million in jewelry given to model Miranda Kerr by Low; and artwork by Picasso and Basquiat valued at more than \$12 million, which Low gave to actor Leonardo DiCaprio.

Ms. Kerr and Mr. DiCaprio have released statements indicating that they are cooperating with the DOJ and will turn over these assets to the U.S. Government.

In total, the U.S. has now brought actions identifying more than \$4.5 billion allegedly stolen from 1MDB, and has sought civil forfeiture of nearly \$1.7 billion in assets traceable to funds it believes were laundered through U.S. financial institutions or are currently present in the U.S. Press reports indicate that U.S. authorities may also be investigating Goldman Sachs’s role in raising billions of dollars for 1MDB through bond issuances. In addition to the U.S., countries such as Switzerland and Singapore also continue to take part in enforcement efforts. Singaporean authorities have brought charges against several bankers who facilitated transactions for the fund, barred certain individuals from further involvement in the country’s financial sector, and levied fines against banks including Credit Suisse and the United Overseas Bank. Switzerland’s investigation into potential money laundering violations tied to 1MDB remains ongoing.

b. Sani Abacha

In August 2014, the DOJ seized more than \$480 million of corrupt funds from bank accounts located around the world of the now-deceased former Nigerian Dictator, Sani Abacha, and his associates under a forfeiture judgement entered by the U.S. District Court for the District of Columbia. The assets seized included \$303 million in two bank accounts in the Bailiwick of Jersey, \$145 million in two bank accounts in France, and an expected \$27 million in three bank accounts in the United Kingdom and Ireland. Additional forfeiture claims involving another approximately \$148 million held in investment portfolios in the United Kingdom are being contested in U.S. courts and remained pending as of September 2017.

According to the DOJ’s unsealed complaint filed in November 2013, Sani Abacha, his son Mohammed Sani Abacha, and his associate Abubakar Atiku Bagudu, among others, embezzled, misappropriated, defrauded, and extorted millions from the Nigerian government and laundered corrupt proceeds through U.S. banks. The DOJ’s complaint identified three main schemes perpetrated by Abacha

and his associates: (i) the systematic embezzling of over \$2 billion in public funds from the Central Bank of Nigeria (“CBN”) under false pretenses of national security; (ii) the purchasing of non-performing government debt from a company controlled by Bagudu and Mohammed Abacha at inflated prices, generating a profit of over \$282 million; and (iii) the extortion of more than \$11 million from a French company and its Nigerian affiliate. According to the complaint, the resulting embezzled funds were laundered out of Nigeria to accounts located in Europe and London through U.S. financial institutions.

National Security: In connection with the first scheme, the DOJ’s complaint alleged that from 1993 to 1998, Abacha directed Nigeria’s National Security Advisor to write over 60 one- to two-page “security votes” letters to the CBN, requesting funds purportedly for national security purposes. Rather than using the more than \$2 billion obtained through these letters for national security expenses, the funds were transferred to the personal accounts of Abacha and his co-conspirators. These fraudulent letters are described as having been endorsed by Abacha, which was contrary to the proper protocol that such letters required approval from Nigeria’s Minister of Finance and Accountant-General.

Government Debt: In the second scheme, the DOJ alleged that Abacha and his associates defrauded Nigeria into purchasing back its own debt at more than twice the market price. The complaint alleges that in 1979, Nigeria agreed to give Tiajpromexport (“TPE”), a Russian company constructing a steel plant in Nigeria, a debt instrument to guarantee payment of \$2 billion to partially finance construction of the plant. Due to a dispute, Nigeria suspended payment on the debt, prompting TPE to stop construction. Abacha’s associate, Bagudu, arranged to purchase the debt from TPE, but only after obtaining a guarantee from the Nigerian government that it would ultimately purchase or repay the debt. The complaint alleges that four months after obtaining the purchase guarantee, TPE sold approximately \$920 million worth of debt to a company named Panar for approximately \$200 million. Panar then immediately resold the debt for approximately \$280 million to Mecosta, a company owned by Bagudu and Abacha’s son. Mecosta then immediately resold the same debt to the government of Nigeria for approximately \$560 million. According to the DOJ, the purchase of the debt by the Nigerian government was approved by Abacha, and as a result, Abacha’s son and his associates gained profits of approximately \$280 million.

French Engineering Company: In the third scheme, Abacha allegedly stopped paying certain foreign government contractors in Nigeria in November 1993. Unable to collect on the \$469 million it was owed by Nigeria, the Dumez Group, a French civil engineering company, agreed to a kickback scheme with the Abacha family in return for payment of the outstanding amounts owed. Dumez agreed to pay 25% of any amounts it received to a company named Allied Network Ltd (“Allied”). From December 1996 through May 1998, Dumez paid \$97 million (25 percent of \$390 million of proceeds it received from Nigeria) to Allied’s Swiss bank account. In late 1997, Mohamad Abacha transferred \$11 million from the Allied account to his personal bank account.

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, and whistleblower complaints, among other legal actions.

1. Derivative Actions

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. These suits typically attempt to prove that the company's board of directors breached its fiduciary duty by failing to implement or adequately monitor internal anti-bribery controls.

Upon filing a derivative suit, a plaintiff must allege with particularity that either (a) the plaintiff has satisfied the demand requirement (*i.e.*, the plaintiff has sent a demand to the board of directors that it immediately cease the challenged behavior or action) or (b) exercising the demand requirement would be futile. Ordinarily, a plaintiff is expected to first notify the board of directors of the demand in writing. However, once a prospective plaintiff undertakes that action, if the board of directors decides not to pursue the shareholder-plaintiff's demand, the board of directors is ordinarily shielded under the business judgment rule from liability. Therefore, many plaintiffs seek to allege that making such a demand would be futile because the board of directors is self-interested in the outcome of such litigation. Courts have required that "a 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 v. Parker*, 803 F. Supp. 2d 630, 640 (S.D. Tex. 2011) (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 of a violation is not sufficient to prove bad faith on the part of the directors. *Id.*

a. Dismissed Cases

Plaintiffs have a heavy burden to shoulder in order to survive a motion to dismiss and pursue their claims successfully. Indeed, courts have regularly noted that "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 fiduciary duties have been dismissed in the past couple of years. For example, 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. After disclosing 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, the company ultimately paid a \$7.5 million penalty to the SEC. The ensuing suit largely relied on evidence obtained from this investigation. In her opinion letter dismissing the suit, Vice Chancellor Tamika Montgomery-Reeves concluded that many of the same warning signs of violations in China allegedly ignored by the board were, in fact, the focus of the company's remedial actions. The Vice Chancellor noted that "no allegations suggest that the Qualcomm

board consciously disregarded the red flags” and that the plaintiffs “simply seek to second-guess the timing and manner of the board’s response to the red flags.”

Och-Ziff Capital Management faced a shareholder derivative 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 their fiduciary duties in relation to the events leading to FCPA investigations by the DOJ and SEC including allegations that: (i) Och-Ziff extended a \$100 million no-interest loan to President Mugabe of Zimbabwe in exchange for access to platinum reserves; (ii) Och-Ziff 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) Och-Ziff entered into a hotel deal for the benefit of Libyan leader Muammar Gaddafi after receiving approximately \$300 million in investments from the Libya Investment Authority sovereign wealth fund. On September 23, 2016, the New York Supreme Court dismissed the case noting in its decision that the board’s demand review committee adequately investigated the shareholder’s complaint over a period of months and, as such, acted in good faith.

Perhaps the most publicized shareholder lawsuits have been filed against Wal-Mart in connection with allegations that it bribed Mexican government officials in order to facilitate the granting of building permits for the construction of its stores in 2005 and 2006 and later sought to conceal the evidence. Following the publication of these allegations in the *New York Times*, Wal-Mart has been mired in litigation, having spent hundreds of millions of dollars on compliance and FCPA-related matters. Proceedings were separately consolidated in the Delaware Court of Chancery and the U.S. District Court for the Western District of Arkansas.

In the Arkansas case, plaintiffs initiated a derivative action against 19 named directors and officers and argued that any demand on the Wal-Mart board to initiate the claims against the named defendants would be futile. The U.S. District Court granted Wal-Mart’s motion to dismiss on March 31, 2015, agreeing with Wal-Mart that the plaintiffs failed to plead with particularity that a majority of the board at the time of the filing of the action lacked independence and was not disinterested. Moreover, although named in the suit, five of the directors were not members of the Board during the relevant period of 2005-2006. Further, the pleadings did not include any particularized allegations on a director-by-director basis as to why the directors that were serving on the board in 2005-2006 would not have been able to exercise disinterested business judgment. On July 22, 2016, the Eighth Circuit affirmed the district court’s dismissal noting that “the allegations do not establish ‘with particularity’” that the threat of personal liability rendered a majority of the board incapable of fairly considering the relevant causes of action.

The Delaware case, which was consolidated on September 3, 2012, initially focused on the production and inspection of relevant books and records pursuant to Del. Code Ann. tit. 8, § 220. On May 20, 2013, the chancery judge heard oral arguments and ruled that Wal-Mart must provide plaintiffs with substantial additional internal files, including all documents in the custody of eleven custodians, certain director-level documents, as well as documents protected by the attorney-client privilege and the attorney work-product doctrine. Wal-Mart appealed, but in a sweeping July 23, 2014 opinion, the Supreme Court of Delaware upheld the Chancery Court’s ruling, finding that all of the categories of documents were “necessary and essential” to the shareholders because they addressed the “crux of the shareholder’s purpose” and were unavailable by other means.

On May 1, 2015, one month after the Arkansas case was dismissed with prejudice, the Plaintiffs in the Delaware case filed a complaint alleging breach of fiduciary duty. This case was dismissed on May 13, 2016, on the grounds of issue preclusion, with the Delaware Chancery Court ruling that the issue of demand futility had been litigated by the Arkansas plaintiffs. In January 2017, the Delaware Supreme Court ordered the Delaware Court of Chancery to more fully consider whether the dismissal of the derivative suit in Delaware on the basis of the Arkansas suit violated the due process rights of shareholders. The *en banc* panel of the Delaware Supreme Court noted that the lack of coordination between the Arkansas and Delaware plaintiffs hurt both. In a supplemental opinion issued July 25, 2017, Chancellor Andre Bouchard of the Delaware Court of Chancery recommended that Delaware adopt a rule that would allow shareholders in derivative suits to continue those actions even if a previous suit making the same allegation was dismissed in another jurisdiction. The Delaware Supreme Court is currently considering Chancellor Bouchard's proposal.

Other FCPA-related shareholder derivative actions that have been dismissed include (i) a shareholder derivative suit surrounding violations of the FCPA by Avon Products, dismissed by the U.S. District Court for the Southern District of New York in May 2015; (ii) a shareholder derivative suit brought against directors of Archer-Midlands-Daniels in the Chancery Division of the Cook County (Illinois) Circuit Court on January 16, 2014, (dismissed by the trial court on December 2, 2015, and appeal dismissed on May 4, 2016); (iii) suits against the officers and directors of Parker Drilling Company by shareholders, filed in Texas state and federal court, alleging that the plaintiff shareholders had not been sufficiently informed that the company was under investigation by the DOJ and the SEC for its use of "customs and freight forwarding agents" in Kazakhstan and Nigeria (with the federal case being dismissed on March 14, 2012, and the state case on July 23, 2012); (iv) a lawsuit filed by a Teamsters' pension trust fund in the Southern District of Texas against current and former officers and directors of Baker Hughes (magistrate judge's memorandum and recommendation of dismissal adopted in May 2010); (v) a derivative claim against current and former directors of BAES by the City of Harper Woods (Michigan) Employees' Retirement System in the U.S. District Court for the District of Columbia (dismissal affirmed in December 2009); and (vi) an ironworkers' pension fund's claim in the Western District of Pennsylvania against current and former Alcoa officers and directors based on the alleged bribes to Bahraini government officials (dismissed in July 2008).

b. Settlements

A few derivative suits, however, have resulted in settlements. Typically, these settlements require the defendant companies to adopt enhanced anti-corruption programs and pay the attorney fees of the plaintiff shareholders.

In September 2017, the petrochemical firm Braskem settled a derivative suit claiming that the value of its American Depositary Receipts fell by more than 20% after disclosure of the firm's involvement in the Brazilian Petrobras scandal. 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 naphtha, an important ingredient in petrochemical processing. The order preliminarily approving the settlement, certifying the settlement class, approving notice to the class, and scheduling the final approval hearing was approved by Judge Paul A. Engelmayer in the U.S. District Court for the Southern District of New York on September 15, 2017.

In January 2014, Georgia-based ATM manufacturer NCR Corporation reached a settlement with a shareholder over allegations that company executives and board members knowingly allowed NCR to violate the FCPA in China and the Middle East, and to violate U.S. sanctions imposed on Syria. The litigation began in 2012 following a story in *The Wall Street Journal* in which a tipster accused the company of violating U.S.-imposed economic sanctions on Syria by continuing to do business in the country. An NCR shareholder subsequently filed a derivative lawsuit in Georgia state court which was then removed to federal court in April 2013. Following several months of negotiations, the parties reached a settlement which provided, in part, that NCR would increase compliance training for its employees and implement a process for tracking company gifts given to government officials, with a special focus on NCR's policies in China. The settlement was approved by Judge Steven C. Jones in the U.S. District Court for the Northern District of Georgia on April 8, 2014. In October 2012, the U.S. District Court for the District of New Jersey approved a settlement in a shareholder derivative case filed against Johnson & Johnson that alleged corrupt practices by Johnson & Johnson in Greece, Poland, and Romania, as well as under the U.N. Oil for Food Program in Iraq. Under the settlement, Johnson & Johnson agreed to (i) adopt and reinforce governance and compliance procedures; (ii) evaluate and compensate its employees on their adherence to those procedures; (iii) fund the governance and compliance reforms for the five-year term of the agreement; and (iv) reimburse plaintiffs' legal fees and expenses up to a cap. An appeal challenging the settlement was dismissed on January 15, 2014.

In June 2012, Halliburton entered into a proposed settlement agreement to resolve shareholder actions brought against it based in part on its alleged involvement in a Nigerian bribery scheme. Litigation began in May 2009 when two pension funds filed separate shareholder derivative suits in Texas state court against current and former Halliburton directors. In January 2011, a Halliburton shareholder submitted a separate demand to the board, alleging essentially the same conduct in violation of the FCPA, which gave rise to the consolidated complaint. Without admitting liability, Halliburton entered into a settlement agreement with plaintiffs, later approved by the Harris County District Court, under which Halliburton agreed to pay the plaintiffs' legal fees and implement changes to its corporate governance policies, which included a revision of its code of business conduct and the introduction of FCPA training.

In February 2012, Maxwell Technologies entered into a proposed settlement to resolve consolidated derivative actions filed by shareholders in connection with allegations that the company bribed officials of a Chinese state-owned electric utility company. Maxwell Technologies agreed to pay \$3 million in attorneys' fees and to adopt enhanced compliance measures. Although the settlement did not require a Mandarin-fluent compliance coordinator, the company did agree to establish a new FCPA and Anti-Corruption Compliance department, which would be spearheaded by a Chief Compliance Officer. In addition to other enhanced governance measures, including due diligence procedures, training, and audit control testing, the settlement agreement also provided for changes to the company's executive compensation policy.

In December 2011, a California state court approved a settlement agreement to resolve consolidated derivative lawsuits against SciClone Pharmaceuticals, which had disclosed previously that it was under investigation by the SEC and the DOJ in connection with its interactions with government-owned entities in China. In addition to agreeing to pay \$2.5 million in plaintiffs' attorneys' fees, SciClone agreed to adopt enhanced corporate governance measures, including: (i) the engagement of a compliance coordinator, fluent in English and Mandarin, who would conduct annual compliance reviews, report directly to the company's audit committee, and file quarterly reports with SciClone's legal counsel,

CEO, CFO, and internal and external auditors; (ii) an enhanced “Global Anti-Bribery & Anti-Corruption Policy” designed to prevent and detect violations of the FCPA and other applicable laws; (iii) maintaining the company’s internal audit and control function; (iv) due diligence reviews in connection with the hiring of all “foreign agents and distributors;” (v) mandatory employee compliance training; and (vi) modifications to the company’s whistleblower program.

2. Class Action Securities Suits

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 Exchange Act and Rule 10b-5, which states that:

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 Section 10(b) or Rule 10b-5, a shareholder plaintiff must plead that the defendant company or directors “made a false statement or omitted a material fact, with scienter, and that plaintiff’s reliance on defendant’s action caused plaintiff injury.” Moreover, the Private Securities Litigation Reform Act (“PSLRA”) established more stringent pleading standards, 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.”

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

In addition, in 2010, the U.S. Supreme Court made it even more difficult for plaintiffs who acquired shares extraterritorially to file claims in U.S. federal courts. In *Morrison v. National Australia Bank*, 130 S. Ct. 2869 (2010), the Court reversed previous federal jurisprudence, holding that Section 10(b) and Rule 10b-5 do not apply extraterritorially. 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.”

a. Notable Dismissed Cases

A number of plaintiffs have failed to meet these stringent standards, including:

-
- Shareholder plaintiffs that 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 Court of Chancery 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);
 - A capital management fund that filed suit following GE's acquisition of InVision, alleging that InVision and its officers had misrepresented that InVision was in compliance with the law before announcing that an internal investigation revealed possible violations of the FCPA, resulting in a drop of the InVision stock price (dismissed by the U.S. District Court for the Northern District of California and affirmed by the Court of Appeals for the 9th Circuit in November 2008);
 - Shareholders who filed suit against Siemens, claiming that that the company had misrepresented the scope and magnitude of the corruption discovered by multiple ongoing investigations (dismissed by the U.S. District Court for the Eastern District of New York in March 2011);
 - Class action plaintiffs who alleged that the stock of SciClone Pharmaceuticals, Inc. ("SciClone") had dropped 40 percent the day it was announced that the SEC and the DOJ were investigating possible FCPA violations related to the company's business in China (voluntarily dismissed by plaintiffs in the U.S. District Court Northern District of California on December 1, 2010);
 - Class action plaintiffs alleging that PetroChina engaged in bribery, political corruption, and undisclosed related party transactions but falsely claimed to have adequate internal controls (dismissed by the U.S. District Court for the Southern District of New York on August 3, 2015 for failing to establish that the underlying fraud occurred during the applicable timeframe and for failing to establish that PetroChina's statements about its compliance practices were false or misleading); and
 - Shareholders who filed suit against Wal-Mart alleging unlawful and unethical conduct in connection with allegations of a bribery scheme at Wal-Mart's largest subsidiary, Wal-Mart de Mexico (dismissed by the U.S. District Court for the Western District of Arkansas on March 31, 2015 for failing to satisfy the requirements for pleading demand futility).

b. Notable Settlement Agreements

Despite the substantial pleading threshold burdens and limitations on extraterritoriality, some plaintiffs have successfully obtained substantial court-approved settlements. Such cases include:

- A class action lawsuit initiated in the U.S. District Court for the Southern District of New York against Avon Products Inc., in which plaintiffs alleged that the company had falsely assured investors that it had effective internal controls and accounting systems (\$62 million settlement in August 2015);

- A securities fraud suit in the U.S. District Court for the Northern District of California against UTStarcom, Inc., which included allegations by plaintiffs of FCPA violations involving the company's activities in China, India, and Mongolia (\$30 million settlement in August 2010);
- An action filed in the U.S. District Court for the District of Utah against Nature's Sunshine Products wherein plaintiffs alleged that the company and several officers made false statements in order to hide serious financial fraud and FCPA violations (\$6 million settlement in September 2009);
- A class action lawsuit in the U.S. District Court for the Middle District of Florida in which plaintiffs alleged that Faro Technologies had overstated sales, understated the cost of goods sold, and concealed its overstatement of profit margins as a result of violations of the FCPA (\$6.875 million settlement in October 2008);
- A securities fraud suit initiated in the U.S. District Court for the District of Texas wherein plaintiffs alleged that Willbros Group inflated its stock price through violations of the FCPA and utilized that inflated stock price to complete a \$70 million offering of Convertible Senior Notes and enter into a \$150 million credit agreement (\$10.5 million settlement in February 2007);
- A securities action filed in the U.S. District Court for the Northern District of Georgia against Immucor, Inc., wherein plaintiffs claimed that the company made false or misleading statements about the scope and gravity of corruption-related investigations in Italy (\$2.5 million settlement in May 2007); and
- A class action lawsuit brought in the Superior Court for the State of California, County of San Diego, against Titan Corporation, in which plaintiff shareholders alleged that the company's FCPA violations prevented it from entering into a definitive merger agreement with Lockheed Martin (\$61.5 million settlement in December 2005).

c. Class-Action Suits Against Brazilian Companies

Following the revelations and allegations that arose in late 2014 in connection with the Brazilian federal police investigation *Operation Car Wash*, investors filed a class-action lawsuit against Petrobras (whose ADRs are listed on the NYSE) on December 8, 2014 in the U.S. District Court for the Southern District of New York.

In the complaint, plaintiffs alleged that Petrobras "made false and misleading statements by misrepresenting facts and failing to disclose a multi-year, multi-billion dollar money-laundering and bribery scheme." The plaintiffs alleged that former Petrobras senior executives received kickbacks from companies operating in the Brazilian oil and gas industry in exchange for inflated contracts. The plaintiffs have attempted to meet the scienter requirements by arguing that Petrobras executives' "knowledge of the fraud is attributable to [Petrobras] for the purposes of assessing [its] scienter."

On February 2, 2016, Judge Jed Rakoff granted a motion by plaintiffs to certify two classes—a class for Securities Act claims under Sections 11, 12(a)(2), and 15 and a class for Exchange Act claims under Sections 10(b) and 20(a)—and also appointing representative parties and class counsel.

Conducting a detailed Rule 23 class-certification analysis, Judge Rakoff concluded that the classes satisfied the numerosity requirement, that there existed common questions of law and fact, that the claims or defenses of the representative parties were typical of the claims or defenses of the class, and that the representative parties will adequately represent the interests of the class. In reaching his decision, Judge Rakoff rejected Petrobras' argument that the high volume of actions brought by individual plaintiffs weighed against the superiority of a class action, concluding instead that the stream of individual actions risked "growing into an unmanageable flood."

Upon appeal, on July 17, 2017, the U.S. Court of Appeals for the Second Circuit remanded the case back to the district court, affirming in part and vacating in part Judge Rakoff's ruling. The Second Circuit affirmed that the district court's class certification analysis passed the ascertainability test under Rule 23 because ascertainability does not require "a showing of administrative feasibility at the class certification stage." The court did, however, vacate the lower court's domestic transactions rationale in its predominance analysis, and remanded the case to the lower court for further analysis.

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 noted the plausibility by investors that they were misled by the company before it revealed that some of its officers were engaged in bribery or bid-rigging. In the decision, he noted that even "as news continued to trickle out about further evidence implicating Eletrobras in the bribery and bidrigging 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, the former Eletrobras CEO, was cleared of all claims of wrongdoing, the court upheld the allegation that two other former officers acted with scienter in making false disclosures to shareholders.

d. Class-Action Suit Against VEON Ltd.

Finally, in contrast to the general trend of shareholder derivative suits being dismissed, 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 Uzbek President's daughter in return for favorable treatment in the Uzbek telecommunications market. Plaintiffs alleged 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 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.

3. 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 countries or state-owned entities implicated in the action. The mere fact that those government entities may themselves have solicited or received the payments in question has not prevented them from bringing suit. Courts, however, have appeared reluctant to allow such entities to bring claims when the foreign entities could themselves be considered co-conspirators in the matter.

Moreover, these types of plaintiffs face the same challenges as more typical shareholders in meeting the stringent pleading standards and the limitation of the application of the securities laws extraterritorially under *Morrison*. But if the foreign government or state-owned entity can survive a motion to dismiss, a substantial settlement can be attained.

For example, on November 4, 2015, Petróleos Mexicanos & Pemex Exploración y Producción (collectively “Pemex”) reached a settlement with Hewlett-Packard Co. (“HP”) and Hewlett-Packard Mexico S. de R.L. de C.V. (“HP Mexico”) to end a lawsuit over HP Mexico’s alleged bribery of Pemex officials. The settlement came after Pemex made statements in a securities filing that seemed to contradict its claims against HP and HP Mexico.

On December 2, 2014, Pemex filed suit against HP and HP Mexico in the U.S. District Court for the Northern District of California alleging violations of RICO and the California Unfair Competition Law as well as fraudulent concealment and tortious interference with contracts in connection with HP Mexico’s alleged bribery of Pemex officials. On April 9, 2014, HP had settled civil charges with the SEC and three HP subsidiaries had settled criminal charges with the DOJ in connection with conduct in Russia, Poland, and Mexico. HP Mexico entered into an NPA with the DOJ that required it to forfeit over \$2.5 million.

As part of the NPA, HP Mexico admitted to paying more than \$1 million in commissions to a consulting company that had close ties to a Pemex official in an effort to win a software sales contract with Pemex. HP Mexico agreed to pay the intermediary an “influencer fee” of 25% if awarded the \$6 million contract. Because the intermediary was not a pre-approved partner and had not been subject to due diligence, HP Mexico instead passed the funds through another previously approved partner that kept a small percentage of the fee.

The District Court initially granted in part the Defendants’ motion to dismiss the suit, ruling that the complaint failed to meet a number of key elements that would give rise to a RICO action. Judge Freeman specifically found that Pemex’s suit failed to allege facts sufficient to show that the pattern of activity in the alleged scheme was domestic. The Plaintiffs also failed to allege a “continuous” pattern of racketeering activity, either internationally or in the U.S., and the alleged activity fell outside of RICO’s four-year statute of limitations. However, the Judge granted Pemex leave to amend its complaint to cure these deficiencies.

In August, 2015, however, the Defendants filed a motion to dismiss the (by then) amended complaint, reiterating many of the same arguments that had led to the partial dismissal of the first complaint and citing to Pemex’s April 2015 SEC Form 20-F, which stated that the Internal Control Body of Petróleos Mexicanos had concluded after conducting an internal investigation that there had been no improper payments by HP Mexico to the former Pemex official. The Defendants chastised Pemex for taking a contradictory position in the litigation, claiming that Pemex was taking “its obligations under Federal Rule of Civil procedure 11 — and to [the] Court — far less seriously than it does its obligations under the U.S. federal securities laws” and arguing that Pemex should voluntarily dismiss its case given the admission. Approximately two and half months later, HP and Pemex settled the case for undisclosed terms.

CHAPTER 3: U.K. ANTI-BRIBERY DEVELOPMENTS

I. Overview

On April 8, 2010, the House of Commons passed legislation to consolidate, clarify and strengthen U.K. anti-bribery law. The 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 (again, 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 U.K. 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 U.K. 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 Considerations Relevant to Investigations

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.

The dispute originated as part of the SFO's criminal investigation into alleged fraud, bribery, and corruption by Eurasian Natural Resources Corporation ("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 ultimately 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 October 2017, Lord Justice Floyd of the Court of Appeal of England and Wales granted ENRC the right to appeal the lower court's decision, reportedly commenting that "the grounds of appeal have a real prospect of success."

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

1. Liberty Media (Formula 1)

In its August 9, 2017 Form 10-Q 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 Parliamentary select committee, asked the SFO to investigate a \$5 million (£3.9 million) payment that the Formula 1 rights holder had made to FIA. The Director of the SFO confirmed in a May 3, 2017 letter to MP Collins that the SFO planned to investigate the matter.

Meanwhile, the 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.

2. 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 two members of the World Health Organization’s Framework Convention on Tobacco Control (“FCTC”), Godefroid Kamwenubusa of Burundi and Chaibou Bedja Abdou of the Comoros Islands, who allegedly received \$3,000 each, as well as former FCTC member Bonaventure Nzeyimana of Rwanda, who allegedly took \$20,000. News reports also allege that BAT paid bribes to Ugandan officials, including \$20,000 to MP Dr. Kasirivu Atwooki in 2012 in order to alter a parliamentary report. Tax authorities and other government officials in Kenya are also suspected of accepting bribes from BAT.

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 August 1, 2017, and BAT has said that it intends to cooperate with the SFO’s investigation.

3. 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.

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 Conté, the government of Guinea originally granted Rio Tinto the Simandou mining concession in the 1990s. However, before President Conté’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 Alpha Condé 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 Condé'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. On that day, an investigative news outlet *Mediapart* published a story about \$10.5 million in payments to François Polge de Combret, a French banker and adviser to President Condé. *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 S. In those emails, Mr. Davies attempted to justify Mr. Combret's large fee by citing Mr. 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 (see *infra*). 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.

4. 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 U.K. prosecutors on 24 February 2014 under the provisions of Schedule 17 of the Crime and Courts Act 2013. A full description of the Rolls Royce case can be found at page 89.

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 Limited ("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 April 10 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 liability 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. Their trial, which is expected to last 13 weeks, began on September 29, 2017. 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. 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 U.K., 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."

7. Unaoil

On July 19, 2016, the SFO announced that it had opened an investigation in March 2016 into Unaoil and its officers, employees, and agents in connection with suspected bribery, corruption and money laundering. The SFO's investigation into Unaoil remains ongoing. Additionally, the probe is connected to the SFO's investigations into several other entities, and has prompted still other companies to conduct their own internal investigations:

- **ABB Ltd** - On February 10, 2017, the SFO announced that it had opened an investigation into the United Kingdom subsidiaries of Swiss engineering company ABB Ltd ("ABB") and related individuals on suspicion of bribery and corruption, noting that this investigation was related to the Unaoil probe. In its Q2 2017 report to shareholders, ABB announced that, in the wake of an internal investigation, it had self-reported to the SFO, SEC, and DOJ "concerning certain of its

past dealings with Unaoil and its subsidiaries, including alleged improper payments made by these entities to third parties.”

- **KBR, Inc.** - On April 28, 2017, the SFO announced that it had opened an investigation into the United Kingdom subsidiaries of American engineering and construction company KBR, Inc. (“KBR”) and related individuals for suspected bribery and corruption, noting that this investigation was related to the Unaoil probe. KBR issued a press release indicating that it had launched an internal investigation into the matter, and that it would cooperate with the SFO, as well as with the DOJ and SEC, which are also conducting investigations into “the same facts and circumstances.”
- **Petrofac** - On May 12, 2017, the SFO announced that it had opened an investigation into United Kingdom oilfield services company Petrofac PLC (“Petrofac”), its subsidiaries, and related individuals for suspected bribery, corruption and money laundering, noting that this investigation was related to the Unaoil probe. In a May 25, 2017 press release, Petrofac announced that it has suspended its COO, Marwan Chedid, and that CEO Ayman Asfari would not take part in any matters related to the investigation. Petrofac also disclosed that in 2016 its board had commissioned an investigation into the Unaoil-related allegations, that it had turned over the results to the SFO, and that the SFO did not accept the findings of the internal investigation. On August 9, 2017, Petrofac announced that it had appointed an outside attorney to serve in an oversight role with respect to the SFO investigation.
- **John Wood Group** - In its May 23, 2017 Prospectus, Scottish energy services company John Wood Group (“Wood Group”) announced that it had launched an internal investigation into its historical relationship with Unaoil in light of the ongoing investigations by regulators. The internal investigation confirmed that a Wood Group joint venture had hired and made payments to Unaoil under agency agreements. An August 2017 update by Wood Group emphasized that, although the investigation had “substantially progressed,” it had not confirmed that the joint venture’s payments to Unaoil were used “in ways that would amount to bribery, corruption or money laundering offences, or that there was any involvement in or knowledge of bribery, corruption or money laundering offences on the part of Wood Group companies, the joint venture or their personnel.” Wood Group further stated that it had disclosed the internal investigation to the Crown Office and Procurator Fiscal Service, Scotland’s relevant authority, and would voluntarily share its findings with the Crown Office.

In addition to discussing Wood Group’s self-directed investigation, the company’s recent disclosures have also mentioned the SFO’s investigation into Amec Foster Wheeler, which Wood Group agreed in March 2017 to acquire for £2.2 billion.

- **Amec Foster Wheeler** - On July 11, 2017, the SFO announced that it had opened an investigation into Amec Foster Wheeler plc (“Foster Wheeler”) and associated entities and individuals for suspected bribery and corruption. The SFO’s announcement follows a previous disclosure by Foster Wheeler that it had been cooperating with the DOJ and SEC in light of their requests for information on Foster Wheeler’s historical use of third parties, particularly in the Middle East. In the same disclosure, Foster Wheeler announced that it had provided the DOJ and SEC with information about operations in other regions, and had made an unspecified disclosure to the SFO.

8. F.H. Bertling Ltd and Related Individuals

The SFO has brought multiple charges against F.H. Bertling Ltd (“Bertling”) and several individuals in connection with making, and conspiring to make, corrupt payments. Bertling is a U.K.-based provider of logistics and project freight operations. Until January 1, 2017, it was also a subsidiary of Bertling Group, a privately-owned multinational headquartered in Germany. The charges arise out of conduct related to freight forwarding contracts in Angola and the North Sea, and are the product of an investigation that began in September 2014.

a. Angola

On July 13, 2016, the SFO charged Bertling and seven individuals for allegedly bribing an agent of Sonangol EP, Angola’s state-owned oil company, between January 2004 and December 2006. The parties stood accused of violating Section 1 of the Prevention of Corruption Act 1906 and Section 1 of the Criminal Law Act 1977. In addition to taking action against the company itself, the SFO also charged Joerg Blumberg, Stephen Emler, Peter Ferdinand, Dirk Juergensen, Giuseppe Morreale, Marc Schweiger, and Ralf Petersen (now deceased) for the same conduct. At the time of charging, Blumberg, Juergensen, and Petersen served as managing directors at Bertling Group, Morreale sat on Bertling’s Board of Directors, and Emler, Ferdinand, and Schweiger no longer worked at either Bertling or its then-parent company.

On September 26, 2017, the SFO announced a series of staggered guilty pleas in connection with the case. Bertling itself pleaded guilty on August 1, 2017. Blumberg, Juergensen, Petersen, and Schweiger pleaded guilty on March 17, 2017. Petersen passed away prior to sentencing. Blumberg, Petersen, and Schweiger were each sentenced to 20 months, suspended for two years, and a £20,000 fine. Morreale and Emler pleaded guilty on September 1, 2017. Sentencing is scheduled for September 2018.

Ferdinand pleaded not guilty and was acquitted on September 21, 2017 by a jury at Southwark Crown Court.

b. The North Sea

The SFO levied additional charges on April 28, 2017, May 3, 2017, and May 17, 2017 against Bertling and various individuals for conspiring to make or accept corrupt payments in connection with oil exploration freight forwarding contracts in the North Sea. All charges again allege violations of Section 1 of the Prevention of Corruption Act 1906 and Section 1 of the Criminal Law Act 1977. The first charge accuses Bertling, Morreale, Emler, and four additional individuals (Colin Bagwell, Robert McNally, Georgina Ayres, and Peter Smith) of conspiracy for actions between January 2010 and May 2013. A second conspiracy charge names Mr. Bagwell, Mr. Smith, and a final individual, Christopher Lane, for activities conducted between January 2010 and December 2010. Bertling Group issued a public statement explaining that all individuals named in the 2017 charges “either never were or are no longer employed by any Bertling entity worldwide” and that Bertling was no longer part of Bertling Group as of the beginning of 2017. Bertling and the individuals appeared at Westminster Magistrates’ Court on May 19, 2017 and were scheduled for an appearance before the Southwark Crown Court on July 27, 2018.

9. DPA with Undisclosed U.K. Company

On July 11, 2016, the SFO announced the approval of its second application for a DPA. Under the terms of the agreement, “XYZ Ltd” (“XYZ”), an undisclosed small to medium sized U.K. enterprise, agreed to pay £6,201,085 in disgorgement of gross profits and £352,000 in financial penalty to the SFO for violations of the Bribery Act, and the Criminal Law Act 1977. The DPA will be effective for at least three years. At the time of the final approval of the judgment, the Crown Court indicated that there were related ongoing criminal proceedings against undisclosed parties.

XYZ was acquired in February 2000 by an unnamed American corporation, ABC Companies LLC (“ABC”), and generates the majority of its revenue from exports to Asian markets. While both companies were unnamed in the judgment, the Preliminary Judgment refers to the “global steel industry,” suggesting that XYZ operates in that sector. Between June 2004 and June 2012, a small but important group of XYZ employees were involved in a systematic bribery scheme relating to 28 contracts in Asia and other foreign jurisdictions. These payments were described in correspondence as fixed, special, and additional commissions to XYZ’s agents, and were made on behalf of XYZ to parties able to exert influence or control over contract awards in the applicable markets. The 28 contracts straddled the commencement of the Bribery Act in 2011, with four contracts postdating the law. Altogether, the bribery scheme resulted in a gross profit of £2.5 million, representing 20.82% of XYZ’s total gross profit over the eight year period.

According to the Crown Court, the misconduct was first discovered by ABC in 2012 during the implementation of a global compliance program within XYZ. ABC took immediate action including the retention of a law firm to conduct independent internal investigations and verbal notification to the SFO. Subsequently, XYZ (i) collected, processed, and searched over 90 GB of electronic data from its servers, (ii) reviewed over 27,000 electronic records, (iii) collected and reviewed hard copy documents such as personal notebooks, agency and contract files, and invoices, and (iv) conducted 13 interviews of four employees. Findings, as well as oral summaries of first accounts of interviews, were submitted to the SFO in three batches. The SFO also seized evidence retrieved from XYZ’s personal email caches, and conducted over 20 interviews of current and former employees and auditors within and outside the U.K. XYZ had facilitated these interviews, and provided timely and complete responses to requests for information of material, subject to what the court described as “a proper claim of legal professional privilege.” Thus, the SFO made clear that the DPA resulted from effective cooperation without waiving legal privilege.

The court considered the role of ABC, finding that it was “entirely ignorant” of the occurrence of the offending activities until discovered. ABC, however, agreed to contribute £1,953,085 of the disgorged amount, representing repayment of a proportion of £6 million received in dividend payments during the relevant period, albeit “entirely innocently.”

In assessing the “interests of justice” element, the Crown Court considered the weight given to the timeliness and completeness of the self-disclosure, which it considered to be integral to discovering the offending activities. XYZ took steps to remediate the reoccurrence of the misconduct including dismissal of two senior employees, termination of seven suspected agents and withdrawal of bids of two suspect potential contracts, which the court considered resulted in a “culturally different company.” The court also found that while the bribe payments were egregious and spanned over an eight-year period, the majority of the bribes had been instigated by the agents and did not reflect an elaborate corporate

conspiracy to hide the payments. In addition, the court found that the evidence did not demonstrate a history of bribery and corruption. Rather, as both XYZ and ABC demonstrated full and genuine cooperation and were in the process of implementing an extensive compliance program, and in the face of XYZ's insolvency risk from a conviction, the court found it likely that the interests of justice would be served with the DPA. During the term of the DPA, XYZ agreed to continue to review, maintain, and report on its compliance program, as well as cooperate with the SFO's related investigations.

10. Peter Michael Chapman (Securrency PTY Ltd.)

On May 12, 2016, Peter Michael Chapman, the former director of business development in Africa for Securrency PTY Ltd. ("Securrency"), was sentenced to 30 months in prison for his role in a scheme to bribe Nigerian officials to obtain contracts to supply the plastic material on which the Nigerian banknotes are printed. Securrency is a Melbourne-based banknote company that is owned in part by the Reserve Bank of Australia. Chapman's conviction was upheld by the Court of Appeal on March 31, 2017. Among other things, Securrency sells a sophisticated polymer compound that can be used in the manufacture of currency to make it more durable and harder to counterfeit than paper banknotes.

Chapman was initially arrested in Rio de Janeiro in late 2014. While awaiting extradition, he spent six months in the notorious Ary Franco prison in Brazil before returning to London in April 2015. Chapman went on trial in the Southwark Crown Court in London in April 2016. Prosecutors argued that Chapman orchestrated a series of bribe payments to Nigerian officials amounting to over \$200,000 between 2007 and 2009, first to induce the Nigerian mint to switch to polymer notes, and then to obtain contracts for Securrency. Prosecutors argued that Chapman passed bribes through a company called Swingaxe, incorporated in the Seychelles. Chapman was found guilty of four counts of making corrupt payments to a foreign official contrary to the Prevention of Corruption Act of 1906, and acquitted on two other counts. In sentencing, the judge noted that Chapman appeared to have been pressured into corrupt practices by his superiors at Securrency and noted the time he had already served in prison, including the difficult six months in Brazil. Based on these factors, Chapman was released at the time of sentencing to serve the remaining sentence on license.

According to prosecutors, other Securrency executives were aware of the scheme, including David Ellery, the former financial controller and company secretary who testified against Chapman in the trial as part of the plea agreement with prosecutors. Ellery testified that he discussed the corrupt scheme with at least three senior executives at Securrency International. According to press reports, Ellery received a suspended sentence on one count of false accounting in return for his cooperation as a witness in other trials.

The SFO alleged that bribes were paid by Deryck A. Gibson, an agent of Mabey & Johnson, to Joseph Uriah Hibbert with the authorization of Mabey & Johnson directors to secure projects and increase project costs. Hibbert served as the Jamaican Chief Technical Director of the Ministry of Transport and Works from November 1993 until October 2000 and had a long-standing relationship with Mabey & Johnson dating back to 1993. While in this position, Hibbert held delegated powers to act on behalf of the Permanent Secretary of the Ministry, which included the ability to enter into financial commitments when there was a vacancy in the Secretary of the Ministry position. During this period, Hibbert received payments of £100,134.62 from Mabey & Johnson. Payments from Mabey & Johnson to

Gibson were originally paid into accounts under Gibson's own name, but later were made to an offshore vehicle.

The primary project at issue was the Priority Flyover Program, known as the "Jamaica 1" contract. In February 1999, Mabey & Johnson entered into a joint venture with Kier International Ltd. for implementation of the Jamaica 1 contract after a presentation was made to the Jamaican Ministry of Transport. Hibbert approached Gibson to make a bid that Hibbert later approved. The contract was valued at £13.9 million but later increased in value to £14.9 million, seemingly as a result of bribes paid to Hibbert. The alleged bribes were paid to Hibbert through commissions paid to Mabey & Johnson agent, Gibson, which were set at an inflated 12.5% rate. In addition to payments made directly to Hibbert, payments were also made to Hibbert's niece and funeral expenses were covered for Hibbert's mother.

According to the Prosecution Opening Note, Mabey & Johnson paid commissions to agents in relation to business it won through the Ghana Development Fund ("GDF"). This fund was to be used for the development of business in Ghana but in actuality was used as a slush fund for Mabey & Johnson to pay bribes. A number of individuals were involved in making and receiving corrupt payments out of the GDF. Consequently, bribes made during the relevant period totaled £470,792.60, which resulted in Mabey & Johnson receiving the award of three principal contracts. These contracts were Priority Bridge Programme Number 1, worth £14.5 million, Priority Bridge Programme Number 2, worth around £8 million, and the Feeder Roads Project, worth £3.5 million. Many of the illicit payments were distributed to members of the Ghanaian government, including Dr. Ato Quarshie, the Minister of Roads and Highways. Mabey & Johnson accepted that in creating and making payments from the GDF, its executives facilitated corruption on behalf of the company and that its executives were in corrupt relationships with public officials in order to affect Mabey & Johnson's affairs.

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, Canada, China, France, and Norway.

I. Brazil

A. *Introduction*

Brazil continues to be a major area of interest in the global fight against corruption, serving as the backdrop for numerous investigations and enforcement actions all over the world. Operation Car Wash continued its aggressive sweep of Brazil's institutions, achieving a record number of convictions and settlements while taking aim at powerful political leaders and economic groups. Operation Weak Flesh uncovered a massive corruption scheme in Brazil's meatpacking industry. Internationally, foreign regulators continued to pursue new cases related to Brazil, supported by Brazil's recent push to increase international cooperation. For example, in connection with Brazil's well-publicized settlement with Odebrecht, several countries where Odebrecht does business (including Peru, Argentina, Mexico, the Dominican Republic, Panama, Colombia, Ecuador, and Venezuela) have requested to share evidence obtained by the Brazilian prosecutors. As of September 2017, the U.S. DOJ and SEC reportedly had at least 35 open investigations with connections to Brazil, including 11 probes into Brazilian companies across various industries (*e.g.*, food, power/energy, oil and gas, steel, air transport, telecommunications, banking).

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.

B. *Enforcement Highlights*

1. Operation Car Wash

Operation Car Wash is the largest anti-corruption investigation 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 September 2017, the snowballing enforcement efforts from Operation Car Wash included: (i) over 1,700 investigations and enforcement actions against companies and individuals related to allegations of bribery, money laundering, and conspiracy; (ii) over 200 arrests; (iii) over 160 settlements

(including leniency agreements with companies and plea bargains with individuals); and (iv) over 300 international cooperation proceedings (including active requests from Brazil to 39 different countries and passive requests received from 30 others). 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 year, 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 no 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 scope of Operation Car Wash. A vote on the second complaint is expected in October.

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 to influence the award of certain Petrobras contracts. He was sentenced to nearly 10 years in prison but remains free pending appeal of his criminal conviction.

In September 2017, Dilma Rousseff (President from 2011-2016), 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.

2. Operation Weak Flesh

In March 2017, Brazilian Federal Police announced the results of an operation investigating corruption in the meat packaging and distribution industry. The probe was dubbed "Operation Weak

Flesh.” According to the authorities, 21 meat companies regularly bribed government inspectors and politicians to approve sales and facilitate exports, even when the meat and poultry was contaminated or spoiled. Alleged bribes ranged from hams, eggs, and leather products to campaign contributions. Over 60 individuals were charged with crimes including corruption, fraud, conspiracy, and forgery of official documents. In the aftermath of the scandal, global markets were briefly closed to Brazilian meat.

One of the many meatpackers implicated was the Brazilian-based company JBS, the largest beef exporter in the world. In May 2017, JBS’s controlling shareholder, J&F Investimentos, finalized a leniency agreement with the Brazilian authorities, agreeing to pay a record BRL 10.3 billion (\$3.2 billion) to settle corruption charges investigated in Operation Weak Flesh and Operation Car Wash. In parallel, seven individuals (including top company executives and external counsel) entered into their own plea agreements admitting to their participation in the scheme. According to court documents, these individuals claim to have made improper payments to nearly 2,000 Brazilian politicians and other public officials over the past 16 years.

C. Anti-Corruption Laws

1. Regulations

Brazil began a complete overhaul of its anti-corruption framework in August 2013, with the enactment of the Clean Companies Act ("CCA") (Law No. 12846/13). Under this new law, 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.

a. 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 has subsidiary jurisdiction over the matter.

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

In light of its new responsibilities, in April 2015, the Ministry of Transparency and Federal Comptroller-General (“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.

2. 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 December 2016, CGU and AGU issued a joint regulation (Interministerial Regulation No. 2,278/16) establishing the procedure to be followed by these agencies in negotiating leniency agreements. Under this directive, companies willing to settle must seek CGU, which will in turn create a joint negotiation committee with AGU. The process concludes with a final report and proposed settlement, which must be reviewed and approved by the CGU Minister and the Federal Attorney-General.

In March 2017, TCU ruled that CGU/AGU should revise certain aspects of this procedure, which were seen as providing excessive benefits to investigated entities. In a separate judgment, TCU refrained from imposing administrative sanctions against companies that had entered into leniency agreements with MPF. The order allowed MPF to amend the settlement conditions and seek full compensation of damages on behalf of the government.

In August 2017, a conflicting decision was issued by a Federal Court of Appeals (4th Region). The court determined that MPF does not have powers to negotiate leniency agreements without the participation of CGU, which has final authority on matters involving damages owed to federal entities. As a result, all leniency agreements previously negotiated by MPF must be reviewed and ratified by CGU. The order noted that, nevertheless, such settlements should involve all enforcement agencies to ensure a proper resolution of the matter in all arenas.

Subsequently, MPF issued its own protocol for negotiating leniency agreements, in part to facilitate coordination with other enforcement authorities (Instruction No. 7/2017). The protocol specifically states that the prosecutors have a duty to liaise with other concerned agencies to seek their participation in each leniency agreement or enable the execution of parallel, compatible settlements. In addition, the rules reflect the TCU recommendation to state that MPF does not have powers to grant companies a full release and discharge of all claims for damages and losses; any payments determined by the settlement on such grounds must be considered as advances, pending further assessment.

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. The heads of CGU, AGU, MPF, and TCU appeared to confirm this tendency, repeatedly calling for enhanced cooperation in this process over the past year.

II. Canada

A. *Overview*

The Corruption of Foreign Public Officials Act (“CFPOA”) is Canada’s implementing legislation to the OECD Convention of Combatting Bribery of Foreign Public Officials in International Business Transactions and the main foreign bribery legislation in Canada. There are essentially two offenses under the CFPOA. It is an offense to bribe or offer to bribe a foreign public official, directly or indirectly, to obtain a business advantage through an act or omission of the official. It is also an offense to create false books and records to facilitate or conceal corrupt payments.

“Foreign public official” is defined broadly under the CFPOA to include officials in legislative, judicial, or administrative positions, individuals performing public duties for a foreign state, and officials of public international organizations.

Overall enforcement of the CFPOA since its inception has been limited. However, the last few years have seen a number of notable success and failures of Canadian prosecutors.

B. Recent Enforcement Actions

1. Cryptometrics

On June 4, 2014, the Royal Canadian Mounted Police charged three individuals with violations under Canada's Corruption of Foreign Public Officials Act ("CFPOA"): U.S. citizens Robert Barra and Dario Bernini and U.K. citizen Shailesh Govindia. All three individuals were connected to Cryptometrics Canada ("Cryptometrics"): Barra and Bernini previously served as the company's CEO and COO, respectively, and Govindia worked at the London-based Emerging Markets Group, serving as an agent for Cryptometrics in connection with its operations in India.

A month earlier, on May 23, 2014, former Cryptometrics India Executive Director Nazir Karigar was sentenced to a three-year prison term for violations of Section 3(1)(b) of the CFPOA. Karigar had been convicted in August 2013 of offering over \$450,000 in bribes to Indian public officials in the form of cash and shares of stock. Karigar had been the first individual prosecuted under the CFPOA.

According to the opinion of Judge Charles Hackland of the Ontario Superior Court of Justice, the alleged misconduct began in June 2005 when Karigar contacted Robert Bell, the Vice President for Business Development at Cryptometrics. Karigar indicated that he had contacts at Air India and was aware that the airline was seeking biometrics technology to improve security at the airline. In September 2005, Karigar arranged meetings for Bell in India with prominent Air India officials. Karigar later provided Cryptometrics with information regarding the expected requirements of Air India and confidential information regarding competitors and proposed tender terms.

In January 2006, Cryptometrics appointed Karigar as Executive Director of the newly established Cryptometrics India. Shortly thereafter, Air India issued an RFP for a biometric facial recognition system and Cryptometrics Canada began to prepare a response. Bell testified in court that Karigar first proposed paying bribes to Indian public officials at a meeting in an Indian hotel to discuss the RFP submission. Karigar then sent Bell spreadsheets listing the Air India officials who should receive bribes, as well as the amount of money and Cryptometrics stock that each should receive. One listing, for example, provided that the Air India Deputy Director of Security—who co-chaired the selection committee for the facial recognition project and who was referred to internally as "the Captain"—should receive company stock and up-front cash.

In June 2006, Karigar sent several emails to Cryptometrics employees, stating that he needed to obtain \$200,000 to pay "the Captain" and that "the Captain" and another individual identified as MMD "need to see the money." Cryptometrics subsequently transferred \$200,000 to Karigar's Mumbai bank account, which was intended to ensure that only two companies were technically qualified for the project.

Karigar, however, also developed the second bid, which he presented under the name of his other company IPCON. In IPCON's bid, Karigar bid the same technology at a higher price in order to create the illusion of a competitive bidding process. In August 2006, IPCON and Cryptometrics were short-listed as the only two qualified bidders. Karigar subsequently explained that Cryptometrics would

win the project because its bid price was lower than IPCON's, so long as it could pay the Minister of Civil Aviation, Praful Patel, an additional \$250,000 to "bless" the system. In March 2007, Cryptometrics entered into a Letter of Agreement with Karigar to provide him with the needed \$250,000.

At some point thereafter, however, it appears that Karigar had a falling out with Barra and Berini, as well as Karigar's principal points of contact in connection with the scheme. Beginning in August 2007, Karigar sent multiple anonymous emails to the DOJ's Fraud Section under the username "Buddy," stating that he had information about U.S. citizens paying bribes to foreign officials and seeking immunity. The DOJ, however, shared Karigar's information with its Canadian counterparts, and the evidence that Karigar himself provided, together with the testimony provided by Bell (who was granted immunity), was used to convict him.

Importantly, Judge Hackland conceded that there was no evidence that Karigar actually paid or offered bribes to Indian public officials. Nevertheless, he ruled that the liability for conspiracy under the CFPOA did not require "proof of the offer of or receipt of a bribe . . . [which] would require evidence from a foreign jurisdiction, possibly putting foreign nationals at risk and would make the legislation difficult if not impossible to enforce and possibly offend international comity." Rather, Judge Hackland stated that it was sufficient that Karigar believed "that bribes needed to be paid as a cost of doing business in India and he agreed with Berini and others to pay such bribes." The Judge also noted that Karigar had told U.S. authorities that he believed that bribes had in fact been paid.

The opinion also states that Barra and Berini continued to seek means to finalize the Air India contract after their dispute with Karigar and that the two executives subsequently hired Govindia of Emerging Markets Group to pay an initial \$2 million to Minister Patel. According to press reports, Patel has claimed that the allegations are baseless and preposterous.

Karigar appealed his conviction arguing, among other things, that (i) there was an insufficient connection to Canada to give the court territorial jurisdiction over what occurred and (ii) for a bribery conviction on the basis of an agreement to pay bribes, the Crown must prove an agreement exists between the accused and the foreign public official.

On July 6, 2017, the Court of Appeal for Ontario affirmed the trial's judge ruling. In rejecting the first ground of Karigar's appeal, the appellate court reasoned that there was sufficient connection to Canada given that the bribery benefited a Canadian company, Karigar was a Canadian who approached a Canadian company, most of the contract work would take place in Canada, all documents and emails that evidenced the transaction were seized in Canada, and all witnesses were Canadian. As to the second argument, the Court of Appeal broadly interpreted Section 3 of the CFPOA to provide no limitation on who must be parties to the agreement, so long as the agreement benefits (or is for the benefit of) the public official. Section 3 states that it is an offense to "obtain or retain an advantage in the course of business, directly or indirectly gives, offers or agrees to give or offer a loan, reward, advantage or benefit of any kind to a foreign public official or to any person for the benefit of a foreign public official."

2. Griffiths Energy

a. Overview

On January 22, 2013, Griffiths Energy International Inc. (“Griffiths Energy”), a Canadian oil and gas company now known as Caracal Energy, pleaded guilty to making an illegal payment of \$2 million to the wife of the Chadian ambassador to Canada in violation of Canada’s Corruption of Foreign Public Officials Act (“CFPOA”). On January 25, 2013, the Court of Queens’ Bench in Calgary accepted a settlement in which Griffiths Energy agreed to pay a fine of CAD \$10.35 million.

According to the Agreed Statement of Facts, Griffiths Energy is a privately held Canadian company that Brad Griffiths, Naeem Tyab, and Tyab’s brother founded in August 2009 in order to purchase various oil blocks in the Republic of Chad. Shortly after the company was founded, Griffiths Energy entered into a consultancy agreement with the Maryland-based Ambassade du Tchad LLC, a company that was wholly owned by Mahamoud Adam Bechir, then-Chadian ambassador to Canada as well as the United States, Brazil, Argentina, and Cuba. The consultancy agreement stated that Ambassade du Tchad would provide various consulting services in connection with Griffiths Energy’s oil and gas projects, and that it would receive a fee of USD 2 million if Griffiths Energy were awarded certain oil blocks by December 31, 2009.

In early September 2009, however, Griffiths Energy’s external legal counsel advised Tyab that Griffiths Energy could not offer to make a payment to Ambassade du Tchad because it was owned by Ambassador Bechir, a government official. Griffiths Energy terminated that consultancy agreement, but several weeks later executed an identical agreement with Chad Oil Consulting LLC, which was wholly owned by Ambassador Bechir’s wife and had been incorporated in Nevada only days prior. Separately, Bechir’s wife and her associates were permitted to purchase 4 million founders shares of Griffiths Energy for a total of CAD \$4,000.

Following a string of MOUs, negotiations, and intensive study of the oil blocks in question between September 2009 and December 2010, Griffiths Energy and the Chadian Ministry of Petroleum and Energy entered into a production sharing agreement on January 19, 2011. On February 8, 2011, Griffiths Energy transferred payment of \$2 million to Chad Oil Consulting’s Washington, DC bank account through an escrow agreement with Griffith Energy’s external law firm.

Griffiths Energy hired an entirely new management team and appointed six new independent directors to its board by September 2011. The new board and management discovered the consultancy agreements while conducting due diligence in anticipation of its Initial Public Offering (which it subsequently withdrew), and it promptly conducted an internal investigation. In November 2011, Griffiths Energy informed Canadian enforcement authorities of the ongoing investigation and also self-disclosed the underlying conduct to U.S. enforcement authorities. Crown prosecutor Robert Sigurdson reportedly told journalists that he expected that the DOJ would not pursue charges given the Canadian prosecution.

The Accepted Statement of Facts praised Griffith Energy’s investigation as being “full and extensive.” Pursuant to the settlement agreement, the company committed to continue to cooperate with the Canadian government, pay a fine of CAD \$10,350,000, and adopt a robust anti-corruption compliance program and strengthen its internal controls.

b. Forfeiture Actions Against Bechir and Wife

According to Canadian newspaper *The Globe and Mail*, Bechir left his post as ambassador to Canada at the end of 2012 and became the Chadian ambassador to South Africa, but he was subsequently dismissed as a result of the bribery scandal. In various interviews and a letter to the newspaper, Bechir asserted that his Maryland-based wife—from whom Canadian authorities are seeking to recover the USD 2 million payment she received as well as her founders shares (now valued at over \$20 million)—had not done anything wrong. To the contrary, Bechir stated that she “deserves her millions” because she legitimately “opened the doors” and convinced the Chadian government to sign the production sharing agreement with Griffiths Energy. Bechir further argued that it was possible that the payment to his wife would not benefit him, noting: “It depends. Not necessarily. I might benefit because she is my wife, but I might not. Maybe she’ll get richer and she’ll be on her own.”

In 2013, Canadian prosecutors filed a forfeiture case against Bechir’s wife and the wife of Youssouf Hamid Takane who was the Deputy Chief of Mission for Chad in the U.S. However, the Chief Federal Prosecutor dropped the charges without explanation in 2014, and the Canadian courts released the freeze order that had been placed on the funds.

In 2014, the DOJ filed a complaint in the U.S. District Court for the District of Columbia to seek the civil forfeiture of nearly \$1.5 million in funds under the U.S. Kleptocracy Recovery Initiative. The DOJ also issued a mutual legal assistance request to the SFO to freeze assets in the U.K. bank account that was linked to the sale of Griffiths Energy stock. The account was frozen and in July 2015, the U.K. High Court upheld a forfeiture order against \$6.8 million, but noted that the judgment was not binding on other jurisdictions because the Canadian courts had not considered the merits of the case.

In June 2015, the DOJ filed a second complaint in the U.S. District Court for the District of Columbia seeking forfeiture of around \$34 million, which is roughly the value of the four million shares in Griffiths Energy that were issued to the wives of Bechir and Takane as well as one other associate. As of October 2017, the case was still pending.

3. SNC-Lavalin Executives

As discussed in detail in Chapter 5, in 2010, the World Bank began an investigation into allegations of corruption surrounding Canadian engineering firm SNC-Lavalin’s bid for the multimillion-dollar Padma Bridge construction project in Bangladesh. After finding credible evidence of corruption, and concerned regarding the lack of cooperation by the Bangladeshi government, the World Bank ultimately withdrew its funding for the project.

In March 2011, a Royal Canadian Mounted Police (“RCMP”) officer approached an investigator at the Vice Presidency for Integrity (“INT”) of the World Bank about possible corruption involving SNC Lavalin and the Padma Bridge project. INT provided the RCMP with email communications from four tipsters about the possible corruption. Based on this information, the RCMP applied for, and was granted, three warrants for wiretaps for two SNC Lavalin executives, Kevin Wallace (Vice-President, Energy and Infrastructure) and Ramesh Shah (Vice-President, the International Division), and a Bangladeshi-Canadian individual, Zulfiquar Bhuiyan (alleged representative of Abul Chowdhury, a senior Bangladeshi

official). Based on the information obtained through the wiretaps, the Crown charged all three individuals in 2013. All three pleaded not guilty.

On January 6, 2017, Judge Nordheimer of the Toronto Superior Court of Justice ruled that the three wiretap warrant applications lacked the requisite grounds for their issuance and therefore evidence obtained from the wiretaps were not admissible at trial. In his decision, Judge Nordheimer reasoned that the tipsters provided “nothing more than speculation, gossip, and rumour” that was “hearsay (or worse) added to other hearsay” that cannot be sufficient basis for the issuance of wiretap warrants. Additionally, in obtaining the warrant, the RCMP did not provide any direct factual evidence to support the rumor and speculation and did not conduct an investigation to verify the statements provided by the tipsters. Judge Nordheimer pointed out that “a tip, by itself, is insufficient to establish reasonable and probable grounds.” Not only that, one tipster provided such general and irrelevant information that in reality, there were only three tipsters, although two should have been treated as confidential informants given that the identify of tipster#1 was unknown, he could have also been the same or different persons as tipster#2 or tipster#3. Judge Nordheimer discussed the ease with which one can create an email account, and unreliable nature of the tips given the nature, source, and information provided, and concluded that the wiretap warrants were issued in violation of the Wallace’s, Shah’s, and Bhuiyan’s right to be free from unreasonable search.

Without the wiretap evidence, the Crown determined that it no longer had a reasonable chance of conviction. The Crown asked Judge Nordheimer to enter a judgment of acquittal.

III. China

2017 marks the fifth year since China launched its anti-corruption campaign, and the fight against corruption remains fierce. According to the Central Commission for Discipline Inspection (“CCDI”), the corruption watchdog for the Communist Party of China (“CPC” or the “Party”), Chinese authorities have received more than 1.31 million complaints and whistleblowing letters, opened 256,000 cases, and punished more than 210,000 officials for violations of Party discipline in the first half of 2017. The majority of these inquiries concerned corruption issues.

Consistent with President Xi Jinping’s zero-tolerance and “no-ceiling” approach (*i.e.* the anti-corruption battle is against all corrupt officials, regardless of their rank or titles: the so-called “tigers” and “flies”), the CCDI and law enforcement bodies in China continue to target corrupt public officials. In the first seven months of 2017, the CCDI investigated at least 12 high-ranking officials. For example, in April 2017, Xiang Junbo, the Chairman of the China Insurance Regulatory Commission, was placed under investigation by the CCDI for suspicion of severe disciplinary violations. Xiang is reportedly the highest-ranking financial regulator ever to come under investigation. According to the Supreme People’s Procuratorate, in the first half of 2017, it opened 12 new cases against corrupt high-level public officials and filed charges against another 14. In addition, 35 high-profile officials were sentenced in the first half of 2017, more than the total number in 2016. Eight of these officials received life imprisonment, including Liu Zhigeng (former vice governor of Guangdong Province), Wang Baoan (former head of the National Bureau of Statistics), and Lu Ziyue (former mayor of Ningbo in Zhejiang Province).

More recently, in a workshop held for provincial and ministerial government officials on July 27, 2017, President Xi stated that while the anti-corruption results since the 18th National Congress of the

CPC in 2012 were satisfying, the Party cannot rest on its laurels in its fight against corruption. President Xi's speech is viewed as a signal that the anti-corruption crackdown will continue in his second five-year term, which will start in late 2017.

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

2017 is the fourth year since the CPC's central inspection teams conducted the first round of inspections on state-owned and affiliated entities and institutions. According to the CCDI, with the 12th round of inspections completed in early 2017, the inspections have reached all provinces, autonomous regions, municipalities, major industries, and major entities in China.

The main purpose of these inspections is to test the reviewed entities' compliance with the Party's integrity and anti-corruption principles. The inspections are conducted by central inspection teams, whose members are selected from various governmental departments and agencies, including the CCDI, the Organization Department of the CPC Central Committee, and the National Audit Office. These inspections, which can take several months to complete, generally comprise the review and analysis of documents (including whistleblower communications) and interviews with relevant staff of the reviewed entities. The findings are subsequently published in summary reports on the CCDI's website.

The CPC has put great effort into these inspections. The inspection teams conducted 53,000 interviews and discovered over 8,200 major violations. The evidence revealed by these inspections accelerated the crackdown on corrupt officials. According to CCDI, more than 60% of all the CCDI's investigations against central officials have been triggered by information gathered by the inspection teams.

Since 2016, the CPC has also been conducting follow-up inspections in major provinces, autonomous regions and municipalities that had previously been inspected. This new feature has not only allowed the CPC to re-examine the risks identified in the past and evaluate the remedial measures taken, but also deterred Chinese officials from acting inconsistently with the Party's anti-corruption principles.

B. *International Manhunt and International Cooperation*

In July 2014, China launched "Operation Fox Hunt," a campaign aimed at repatriating economic crimes 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.

Many key 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 Supreme People's Procuratorate, 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 Supreme People's Procuratorate 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"), also released a "100 most wanted" list of Chinese fugitives. The list includes the suspects' photos, identification and 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 May 31, 2017, through Operations Fox Hunt and Sky Net and cooperation with Interpol, China has recovered RMB9.10 billion (approximately \$1.37 billion) and repatriated 3,051 fugitives from more than 90 countries and regions. Forty-three fugitives on the most wanted list have been returned to China.

Aside from cooperating with Interpol, China also reinforced its ties with law enforcement agencies of individual countries where some of the fugitives were hiding. 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 now successfully ratified treaties with several European countries, including France, Portugal, and Italy.

Even where no extradition treaties exist, China has been actively increasing its law enforcement cooperation with foreign nations. As of August 7, 2017, China has established various types of law enforcement cooperation arrangements with approximately 200 countries. For example, in September 2016 China and Canada signed three law enforcement agreements: (i) an agreement for sharing and return of forfeited assets; (ii) an agreement on cooperation between border agencies; and (iii) an MOU between the Royal Canadian Mounted Police and the Ministry of Public Security in China on combating crime.

The increased collaboration between China and its international counterparts has reduced the difficulty for China to hunt down fugitives, even those hiding in countries with which China has no extradition treaties. For example, in June 2017, despite China not having an extradition treaty with Canada, a Chinese economic fugitive living in Canada was returned to police in Shanghai as a result of the cooperation in law enforcement and fugitive repatriation between China and Canada. Similarly, on November 17, 2016, China's most wanted corruption suspect, Yang Xiuzhu, was repatriated from the United States after 13 years on the run. Yang was accused of embezzling \$39 million while working as deputy director of the construction bureau in the eastern city of Wenzhou.

Since 1998, China and the United States have held meetings of the China-U.S. Joint Liaison Group ("JLG") on Law Enforcement Cooperation. Through the JLG, the United States and China have worked closely to apprehend Chinese fugitives in the United States. Despite the lack of an extradition treaty, the United States has indicated its willingness to repatriate Chinese citizens if provided credible evidence of their crimes. Chinese and U.S. officials indicated that China provided the U.S. with evidence of Yang's crimes prior to her repatriation in 2016.

C. *Creation of National Supervisory Commission*

In January 2017, China announced that it will create a “National Supervisory Commission” (NSC) to reform the state supervisory system. State supervisory functions with respect to auditing, inspection, and discipline that have historically resided in the CPC, state administrative bodies, and state judicial bodies will be integrated into the NSC. Beijing, Shanxi, and Zhejiang were selected to pilot the reform, which involves the trial establishment of local supervisory commissions at provincial, municipal and county levels. The lessons and experience gathered in the pilot reform will be reflected in the ongoing revision of the law on administrative supervision. The law is expected to be finalized by March 2018 and will provide legal support for launching the reform in all areas in China.

Unlike the CCDI, which is an anti-corruption body within the Party, the NSC’s power comes from China’s National People’s Congress (the law-making authority in China). Therefore, the NSC will have more independence and power in supervising and disciplining public officials. Since the beginning of the anti-corruption campaign, CCDI has been playing a major role in the hunt for corrupt Party members. However, this also raised concerns over CCDI’s opaque investigation process and the possible use of excessive violence in interrogations, which do not necessarily strictly abide by relevant laws and procedures. In the pilot reform, the supervisory commissions of various levels are given 12 types of powers, including inquiry, examination, asset freezing, and detention. While these powers are not new compared to those that are now held by CCDI and other bribery-handling agencies, by such recognition they have become more transparently legitimate powers and the enforcement of such powers is now strictly controlled by law. For example, Shanxi NSC has set a 90-day cap on the length of detention and adopted a series of procedures for the execution of its powers.

It is possible that the NSC will take on a critical role in China’s anti-corruption battle. Within half a year, the Shanxi NSC alone has interviewed 5,652 people, frozen the assets of five people, searched the premises of ten people, and detained nine people for investigation.

D. *Legislative and Regulatory Development*

In 2016 and 2017, China enacted and proposed several new laws and regulations that brought substantive changes to the Chinese anti-corruption environment. These laws and regulations broadened the scope of corruption-related offenses and placed an increased responsibility on market players to prevent instances of corruption.

China’s Anti-Unfair Competition Law (“AUCL”) regulates various forms of unfair practices including commercial bribery. The current AUCL was implemented in 1993 and has not been updated since. Last year, the Legislative Affairs Office of the State Council in China submitted the revision draft to the AUCL for public comments. In February 2017, another version of the draft amendments (“2017 Amendments”) was released for public comments after being reviewed by the standing committee of the National People’s Congress.

Compared to the current AUCL, the 2017 Amendments reflect a number of changes on issues concerning the modern business climate, including protection of trade secrets, internet-related unfair competition, powers of the administrative enforcement authorities, and commercial bribery. Some key features proposed in the 2017 Amendments are outlined below.

Bribes to third parties are prohibited. While the current AUCL only prohibits bribery between the parties to a transaction, the 2017 Amendments proposes to regulate third parties as well. Article 7 of the 2017 Amendments 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 2017 Amendments as an entity or individual with authority to influence the transaction.

Vicarious liability for the employer. The current AUCL does 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 has benefited the company.

The recent amendments to the AUCL create a rebuttable presumption that a company is liable for the corrupt conduct of its employees except when it can demonstrate that an employee violated the employer’s interests through the corrupt conduct. The 2017 Amendments would clarify the rule by stating that “where business operators’ employees use bribery to seek trading opportunities or competitive advantages for the business operator, such acts shall be deemed to be the acts of the business operators, except where the business operator has evidence showing that it was an individual conduct.” If this proposal is adopted in the final version of the AUCL, entities in China will have liability for the acts of their employees, thus placing a heavier burden on training employees and exercising control over employees’ actions.

Fines and penalties. For commercial bribery, the AUCL currently imposes a fine ranging from RMB10,000 to RMB200,000 (approximately from \$1,500 to \$3,000), as well as confiscation of illegal income resulting from the bribery. Because inflation has increased over the past two decades, such fines have little, if any, impact on discouraging market players from engaging in corruption. In the 2017 Amendments, the range of the monetary fines is raised to a range of between RMB100,000 to RMB3,000,000 (approximately \$15,000 to \$435,000). While the 2017 Amendments would remove the penalty of confiscation of illegal income, it would add revocation of a business license as a penalty in serious cases.

E. First Anti-Bribery Standards for Organizations in China

In June 2017, the city of Shenzhen, China’s fourth largest and wealthiest city, published the Anti-bribery Management System Shenzhen Standards (“Shenzhen Standards”). The Shenzhen Standards follow the ISO3700 standards on anti-bribery management systems. ISO 3700, which was developed in late 2016 by an ISO committee with members from 61 countries, represents a global consensus on best practices for organizations to manage anti-corruption compliance.

The Shenzhen Standards became effective on July 1, 2017. As the first of its kind implemented in China, the Shenzhen Standards provide guidelines in various areas in anti-corruption practices. The Shenzhen Standards set compliance management standards in areas including:

- Top management involvement and leadership;
- Anti-bribery staffing;
- Anti-bribery policies and procedures;

- Training for internal employees and third parties;
- Third party due diligence and risk assessment;
- Financial and non-financial (*e.g. screening, procurement, and contractual*) controls; and
- Reporting, monitoring, auditing, and investigation procedures.

Under the Shenzhen Standards, an organization is expected to provide induction training and follow-up training to its employees regarding its anti-bribery policies and procedures. An organization following the Shenzhen Standards also must familiarize business partners with the organization's anti-bribery requirements and obtain compliance commitments from such business partners unless they are deemed low-risk. The organization should also maintain whistle-blowing procedures to encourage employees to report suspected bribery and allow them to do so anonymously. In addition, the organization must conduct periodic internal audits and self-evaluations to constantly monitor the compliance system.

The Shenzhen Standards represent the first effort by a Chinese government principality or agency to explain what is expected from organizations regarding anti-corruption compliance. Although the Shenzhen Standards are not compulsory, according to the Shenzhen government, more than 60 entities have participated in the pilot program and agreed to adopt the standards. Participating entities include some major Chinese corporations such as Vanke (a leading real estate developer in China), ZTE (a large company focusing on telecommunications equipment and systems), and China International Marine Containers Co., Ltd. Local officials have also indicated that entities that fully adopt the Shenzhen Standards will be given preference in bidding for procurement contracts, projects, and government funding.

IV. France

As 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, has 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. *France's History Combatting Corruption*

In the 1990s, the rise of market-based economic models and more open societies spurred a climate of increasing transparency and accountability. In response, governments and international organizations became interested in enacting anti-corruption legislation to decrease the cost of business and market distortions. In this vein, France signed several international conventions in an effort to combat corruption. For example, France became a State party to the following conventions:

- **The European Union Convention against Corruption Involving Officials** (“EU Convention Against Corruption” - signed by France on May 26, 1997, and entered into force on September 28, 2005) which requires EU Member States laws to (i) punish acts of passive or active corruption as a crime and (ii) permit the heads of businesses or those exercising control within a business to be declared criminally liable in cases of active corruption by a person acting under their authority on behalf of the business;
- **The OECD Convention on Combating Bribery of Foreign Officials in International Business Transactions** (“OECD Convention” - signed by France on December 17, 1997 and ratified on July 31, 2000) pursuant to which signatories must take measures to establish as a criminal offence under their laws for any person intentionally to offer, promise or give an undue pecuniary or other advantage, whether directly or through intermediaries, to a foreign public official or for a third party, in order that the official act or refrain from acting in relation to the performance of their official duties;
- **The Criminal Law Convention on Corruption of the Council of Europe** (dated January 27, 1999, signed by France on September 9, 1999, and entered into force on July 1, 2002) which reproduces the definition and the general outline of the OECD Convention while supplementing it significantly, including by encompassing both active and passive as well as private and public corruption and influence peddling. This Convention defines the acts that must be criminalized and requires the signatory States to provide for efficient and dissuasive measures, including sanctions involving deprivation of liberty for natural persons and sanctions applicable to legal entities.
- **The Civil Law Convention on Corruption of the Council of Europe** (dated November 4, 1999; signed by France on September 26, 1999, and entered into force on November 1, 2003) which requires signatories to provide in their domestic laws effective remedies for persons who have suffered damage as a result of acts of corruption, in order to enable them to defend their rights and interests. Specifically, it requires member states to provide procedures to obtain compensation for damage resulting from corruption by its public officials.
- **The United Nations Convention Against Corruption** (UN Merida Convention” - signed by France on December 9, 2003, and entered into force on December 14, 2005) , which is the first legally binding global instrument to address preventative measures, criminalization and law enforcement, international cooperation, asset recovery, and technical assistance and information exchange. The UN Merida Convention requires the signing countries to adopt measures aimed at detecting corruption involving the private sector and to enhance accounting and auditing standards in the private sector and, as the case may, to provide effective, proportionate and dissuasive sanctions, be they civil, administrative or criminal, in case of failure to comply with these measures. Measures to achieve these ends may include promoting the developing of business codes of conduct, best practices, and compliance programs. In addition, under the Convention, the signing countries shall adopt measures to establish the liability of legal persons. Furthermore, under the Convention, signatories are to adopt a variety of anti-money laundering preventative measures, and to adopt mechanisms for the recovery of property through civil lawsuits.

In December 1997, following France's signature of the OECD Convention, France passed legislation (under Article 39-1 of the French Tax Code) prohibiting the tax deductibility of bribes paid to foreign officials. As originally enacted, the legislation only applied to contracts entered into after the entry into force of the OECD Convention and might thus have allowed tax deductibility to continue for previous contracts. Responding to criticism by other OECD members, the French Parliament enacted a law in February 2000 to extend Article 39-1 provisions to any contract.

In June 2000, just before France's ratification of the OECD Convention and years after having criminalized the bribery of domestic officials, French legislators implemented regulations that prohibited the bribery of foreign public officials. Criminal Act No. 2000-595 of June 30, 2000, which modified the French Penal Code by, *inter alia*, adding to it a new Article 435-3, made it a criminal offence to proffer at any time, without the right, directly or indirectly, any offer, promise, donation or gift or advantage of any kind to a person holding public office, discharging a public service function or holding an electoral mandate in a foreign State or within a public international organization, either for his/her own benefit or that of a third party, for the purpose of carrying out or abstaining from carrying out an act of his function, duty or mandate. This law also penalizes any person as defined above who solicits, without right, at any time, directly or indirectly, any offer, promise, donation, gift or advantage, either for his own benefit or that of a third party, of any kind with a view to carrying out or abstaining from carrying out an act referred to in the previous paragraph.

In its Phase 1 Report issued in 2000, the OECD Working Group on Bribery acknowledged that France had incorporated the OECD Convention requirements by enacting Criminal Act No. 2000-595 and new Article 435-3.

In January 2004, when the OECD Working Group on Bribery issued a Phase 2 report, it recommended that France implement several recommendations, including that it should (i) encourage small and medium enterprises to implement internal control mechanisms; (ii) issue regular anti-corruption reminders through official channels; (iii) make financial and professional organizations which are subject to the obligation to declare suspicious transactions to TRACFIN (the financial intelligence unit) more aware of the provisions of the above mentioned Criminal Act No. 2000-595 and to apply sanctions effectively, (iv) adopt mechanisms for the effective prosecution of bribery of foreign officials, including by extending the statute of limitations for the offense of foreign bribery of public officials to ensure adequate time to prosecute the offence; and (v) notify magistrates of the importance of effectively applying criminal liability for the bribery of foreign public officials and encourage them to impose the penalty of confiscation. In 2006 and 2012, the OECD Working Group provided France with a series of additional recommendations to implement the OECD Convention.

In 2013, France addressed some of these recommendations by *inter alia* (i) creating a new prosecutors office with special jurisdiction over economic and financial crimes (the "Parquet National Financier" or "PNF"), (ii) increasing financial penalties for corruption offenses from 150,000 euros to 1 million euros or double the proceeds of the offence (whichever is greater); (iii) introducing protections for certain corruption whistleblowers, and (iv) opening up the possibility for anti-corruption organizations to bring civil party claims. Despite efforts to refine its anticorruption landscape, the OECD Working Group on Bribery reported serious concerns regarding the lack of foreign bribery convictions in France.

In its 2014 report, following a comprehensive review of France's implementation of its anti-corruption legislation, the OECD Working Group determined that France had failed to implement a number of its recommendations. For example, the Working Group noted that while the French Minister of Justice had committed to adopting changes to its criminal policy (including reforms which would give public prosecutors statutory support to exercise their functions without undue political influence), France failed to implement these reforms. France had also failed to enact other anti-corruption reforms, including ensuring that French blocking statutes were not used to prevent the investigation and prosecution of foreign bribery cases, and extending the statute of limitations for prosecutors to bring charges of corruption.

B. Sapin II

Under international pressure to comply and implement its obligations under the OECD Convention, France enacted a series of reforms targeting transparency and corrupt activities. 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) criminalizes the influence peddling of foreign officials, (ii) extends French jurisdiction over certain corruption related offenses, (iii) creates a version of a deferred prosecution agreement ("DPA"), (iv) creates the *Agence Française Anticorruption* (French Anticorruption Agency, or "AFA"), (v) requires companies of a certain size to adopt and implement anti-corruption compliance programs, (vi) introduces a new criminal penalty through the court-imposed monitorship, (vii) provides additional protections for whistleblowers and (viii) imposes 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 the following penalties of up to 5 years' imprisonment and a maximum criminal fine of 500,000 euros 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 euros).

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 US Foreign Corrupt Practices Act and the UK 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 should allow French prosecuting authorities to have 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 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 mouvement") 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 which has been put under investigation needs to acknowledge the alleged facts and agree to their proposed legal characterization. In any case, the CJIP will include (i) a public interest fine that will be proportionate to the gains made from the breach, without exceeding 30% of the entity's average annual turnover on the last three years; (2) the implementation of a compliance program under the supervision of the AFA, for a maximum of three years; and (3) 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 or does not satisfy the terms of the agreement, then the prosecutor moves forward with the prosecution, absent new facts. 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.

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. To date, the one attempted CJIP offered to UBS for settling a case of tax fraud, has been refused by the bank which considered the proposed fine, 1.1 billion euros, to be excessive

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, 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*).

Sapin II further provided that the AFA may issue tailored recommendations that will be regularly revised in light of practices 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, including actions that impose 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*, 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 on-site 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. Importantly, 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 offences 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 Euros, and on companies of up to 1 million Euros. 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 to 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 being noted 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 adopt 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 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 euros, 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 euros. 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. 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, recommendations 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. 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.

d. AFA's Recommendations on the Compliance Program

On October 4, 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:

- o Code of Conduct: The AFA recommends that the code of conduct:
 - i. be based on risks identified during a risk mapping exercise and that these risks serve as the starting point for a description of prohibited situations and conduct;
 - ii. contain provisions describing prohibited conduct involving gifts and hospitality, facilitation payments, conflicts of interests (lobbying) as well as donations and sponsoring;
 - iii. define the disciplinary consequences for violation of the code and specify the mechanism(s) to report possible violations of the code;
 - iv. apply to all employees, external staff and temporary workers and be applied in relationships with clients, suppliers and partners, including those outside of France;
 - v. be updated regularly, particularly following a new risk assessment.
- o Risk Assessment: According to the AFA, the risk assessment requirement of Sapin II has a dual objective. It is first intended to identify, review, rank and manage the corruption risk to guarantee that the company's compliance program is efficient and adapted to its economic model. For the AFA, a risk assessment has three main features; it is (i) "exhaustive and precise"; (ii) formalized and accessible and (iii) adaptable over time to

changing risks. In its guidance, the AFA suggests that all employees can play a role in the risk assessment exercise, but does not provide greater details on how this would operate in practice. AFA guidance on risk assessments provides that the risk assessment process should include the following six steps:

- i. define the roles and responsibilities in the creation, implementation and review of the risk assessment. Management decides to conduct a risk assessment, and the compliance officer, who should have functional independence from management, leads the implementation and review of the compliance program. The compliance officer would typically lead the risk assessment and share its results with management, who in turn formally approves the risk management strategy on that basis. Management is also responsible for ensuring the implementation of the risk assessment's action plan;
- ii. identify the risks inherent to the operations of the company. This step of the risk assessment is intended to draw up an inventory of documented and particularized risk factors, including those arising out of due diligence on third parties. The AFA refers to this portion of the risk assessment exercise as the review of "net risks".
- iii. assess the company's exposure to each identified corruption risk. That analysis is done using two data points (i) the probability of occurrence (for instance, based on the history of incidents) multiplied by aggravating factors, such as a particular industry or activity, or the implication of third parties. As described by the AFA, this step focuses on "residual risks" ;
- iv. review the appropriateness and the efficiency of the means intended to manage these risks. The AFA recommendation notes that this stage of the risk assessment seeks to identify the level of control that the organization has over the identified net and residual risks;
- v. rank and address both net and residual risks. Once these risks have been identified, management should rank the risks, distinguishing between manageable and unmanageable risks. Once what is referred to as "the limit of acceptability" is defined in a procedure annexed to the risk assessment, the company should, in the framework of the risk management strategy, determine the measures that need to be taken to adjust the corruption prevention program and limit the probability of occurrence or lack of aggravating factors. A plan is agreed upon on that basis.
- vi. formalize the risk assessment and keep it up-to-date. The AFA provided some guidance on the form that the risk assessment should take. The documentation may be organized by function (*métier*) or process. An annex should describe how the risk assessment was prepared and conducted and how the risks were characterized. The need to review the risk assessment should be considered annually. According to the AFA, in any case, the risk assessment must be reviewed in light of the evolution of the business. Among the events that would prompt the need to review the risk assessment are changes in the economic model or

processes, a new organization, mergers of acquisitions, or significant changes in the regulatory or economic context.

- **Internal Reporting Mechanism:** Under Sapin II, companies should implement an internal reporting mechanism allowing employees to flag behavior or potential violations of the code of conduct. Per AFA's recommendation, the internal reporting mechanism is intended to identify conduct that is contrary to the code of conduct in order to (i) end it, (ii) sanction the individual(s) responsible as the case may be, and (iii) update the risk assessment to avoid future occurrence of similar conduct. The AFA recommends that companies:
 - Guarantee the confidentiality of the identity of the person alerting the company to a potential violation and of the persons affected by the alert;
 - Open the reporting mechanism to individuals outside of the company; and
 - Communicate the creation of the whistleblower program, its protections and its accessibility.

The AFA has stated that it expects to release a second set of recommendations in November 2017, which would include: (i) recommendations for third-parties due diligence procedures; (ii) recommendations on accounting audit procedures; (iii) recommendations on the implementation of anti-corruption training mechanisms; and (iv) recommendations on the evaluation and monitoring of compliance measures.

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 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.

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. 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,” 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. 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 denouncing, French law introduced incremental protections and rules for whistleblowers. While the protection system progressively introduced by law was disseminated throughout various statutes 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.

It is worth noting that contrary to the US Dodd-Frank whistleblowing provisions, the French whistleblowing system is contrary to 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 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, and 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. Lobbyists are defined under French statute as (i) any natural person as well as (ii) any private or public company employing persons whose main activity is to influence public decision, in particular on 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;
- His/her/its acts in lobbying as well as the amount of expenses related to those activities in the previous year;
- The number of persons his/her/it employs 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 to a fine of up to 15,000 euros and imprisonment of up to one year. The HATVP has the power to request documents and to conduct on-site 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. In fact, 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 euros and 300,000 euros, respectively. The decision has been appealed before the *Cour de Cassation*, France’s highest court, but at the time of this writing, the effect of the appeal was not known. 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 euros fine. However, on January 7, 2015, the Paris Court of Appeals overturned this decision, and Safran’s conviction was overturned.

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 subcontractor. The bill received strong popular support since it was proposed in response to a series of human rights violations committed by large companies, and 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 (1) a risk mapping intended to identify, analyze and rank the risks, (2) due diligence and risk assessment procedures to be conducted on subsidiaries, subcontractors and suppliers; (3) appropriate actions of risk mitigation and prevention of serious breaches; (4) a whistleblowing report procedure allowing the collection of relevant information in light of the risks targeted and (5) a follow-up 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, imposed a fine (*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 euros or 30 million in the event of a severe breach of the fundamental rights protected by the Law. However, 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 profession 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 services companies, but also non-financial services companies trading fine stones, fine metals, jewels, furniture and interior decorative items, cosmetics, textile products, leather goods, fine food, clocks and tableware, accepting payments in cash above a certain amount yet to be set by decree. 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 law 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 the 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 euros and 5 million euros 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, or control of executive bodies of the company, or 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, and must provide this information to the commercial registry upon registration, and then 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 2016, 64,815 “pieces of information” were transmitted to TRACFIN, as well as 62,259 reports of suspicious activity, amounting to a 44% increase since 2015. TRACFIN conducted investigations or posed further questions on 13,592 of those reports in 2016 (a 28% increase compared to 2015), and 1,454 investigation requests were sent to foreign investigatory counterparts. TRACFIN sent 1,889 files to

French judicial and administrative authorities for further action based on its analysis of reports of suspicious activity.

In December 2016, TRACFIN's powers were expanded, which allows to believe that the statistics will get higher next year. For instance, TRACFIN is now vested with the authority to identify to any entity subject to its reporting obligations 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 transaction 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.

V. Norway

In the past few years, Norway has seen an increase in anti-corruption enforcement efforts and focus on compliance. Stakeholder enforcement initiatives have continued to gain momentum. At the forefront of this trend is the Council on Ethics for the Government Pension Fund Global, which 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. Interestingly, the Council has set the tone for other important stakeholders. For example Kommunal Landspensjonskass ("KLP"), Norway's largest insurance company, excluded at least two companies from its portfolio on the basis that these had been recommended for exclusion by the Council on Ethics. Such stakeholder enforcement is contributing to shaping (and elevating) 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. **Enforcement Focus: Yara International**

1. 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 (holding 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 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, 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.

2. 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 Business 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 payments were made in order 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 acts of corruption were carefully planned; and (v) Wallace was the Legal Director, member of Yara's senior management and oversaw 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," qualifying the fact that Wallace was personally involved in serious acts of corruption, "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 to 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.

3. 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 the 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 Wallace's own prominent position as the Legal Director, who by virtue of his position, skills and power could have refused to aid and abet to the acts without any risk to his own position. The Court also pointed to Wallace's central role in the planning and executing the corrupt scheme. Wallace decided that the agreement should be oral and took the initiative to making 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 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 toward a key public official. Again, Wallace was central in the corruption scheme; 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.

The Supreme Court rejected two of Wallace's key arguments: (i) that the prosecution failed to establish that the acts of corruption caused any negative consequences or harm; and (ii) that the underlying agreements relating to the production of fertilizers was of great national importance for both Libya and India. The Supreme Court reiterated that the purpose of the payments was to obtain favorable treatment of Yara and to improve Yara's prospects of being able to sign the deal. The Supreme Court cited previous case law, which states that the risk of harm, not actual harm, is relevant for purposes of the foreign bribery analysis. In corruption cases, harm is not limited to the direct financial effects, but also indirect harm such as breaches of trust and loss of reputation. Finally, the Court categorically rejected as irrelevant the contention that the underlying agreements relating to the production of fertilizers could be of national importance for Libya and India should be viewed as a mitigating factor.

For 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.

B. Other Investigations and Actions of Note

1. Sevan Drilling ASA

In October 2015, Sevan Drilling ASA ("Sevan Drilling"), an international drilling contractor specializing in ultra-deepwater operations, listed on the Oslo Stock Exchange and controlled by Seadrill, was charged with gross corruption in connection to alleged payments of bribes to Petrobras officials in connection with the award of Petrobras drilling contracts to Sevan Marine ASA ("Sevan Marine") between 2005 and 2008.

At the time of the conduct in question, Sevan Drilling was 100% owned by Sevan Marine. However, in 2011, Sevan Marine underwent restructuring. As part of the restructuring process, Sevan Drilling was spun-out and listed separately on the Oslo Stock Exchange. Following the restructuring, Sevan Drilling gained control of two rigs that had long-term contracts with Petrobras.

On June 29, 2015, following allegations in the Brazilian press that Sevan Marine had made improper payments through its former Brazil Managing Director Raul Schmidt Felipe, Jr. to obtain the Petrobras contracts, Sevan Marine and Sevan Drilling issued separate Oslo Stock Exchange Notices indicating that Sevan Drilling had hired a Norwegian law firm to conduct an investigation of the allegations. On October 16, 2015, Sevan Marine disclosed that its Board of Directors had received the investigation report relating to the facts and circumstances surrounding the awards of contracts by Petrobras, and that the report concluded that “illegal conduct occurred in the form of improper payments to obtain business when Petrobras awarded contracts to Sevan Piranema, Sevan Driller and Sevan Brazil during the relevant period,” and that there were “indications of suspicious acts and transactions, constituting both a neglect of Sevan’s affair and/or a conflict with Sevan’s interests and such acts may potentially represent economic crime.” Sevan Marine indicated that the report had been transmitted to ØKOKRIM and that the Board of Directors had also initiated early contact with the relevant prosecutor’s offices in the other concerned jurisdictions (US, UK and Brazil).

Days after the notice, ØKOKRIM confirmed that its investigators had raided the offices of Sevan Drilling at several locations in Norway seizing important volumes of documents and data relating to the circumstances surrounding use of agents and contracts in Brazil. ØKOKRIM later confirmed that it was investigating Sevan Drilling and its founder Arne Smedal for breaches of §§ 276(a) and (b) of the Norwegian Criminal Code (now §§ 387 and 388 of the new Norwegian Criminal Code)

While the charges are not public, according to Brazilian and Norwegian news reports, Sevan is suspected of having paid at least USD 20 million in bribes between 2012 and 2015 through Raul Schmidt Felipe, Jr. The payments were allegedly made through the Swiss bank Julius Baer to accounts controlled by Mr. Jorge Luiz Zelada, former head of Petrobras’ International Division. Mr. Schmidt Felipe, Jr. led Sevan’s activities in Brazil until 2007, after which he established his own consultancy company and acted as a consultant in connection with the three contracts Sevan Marine concluded with Petrobras. In June 2017, ØKOKRIM announced that it was dropping the charges against Arne Smedal. ØKOKRIM has not yet confirmed when it will make a charging decision with respect to Sevan Drilling. The current investigation involves several countries, including Switzerland. Brazil has sought to extradite Raul Schmidt Felipe Jr. from Portugal in connection with charges of corruption, money laundering and conspiracy. On September 8, 2017, the Portuguese Supreme Court confirmed the Appeals Court’s decision to extradite Schmidt to Brazil, on condition that he could only be judged for facts prior to 2011, the date upon which Schmidt obtained Portuguese nationality.

2. Statkraft

In March 2017, Statkraft AS, a Norwegian fully state-owned hydropower company disclosed that it has 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”). 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. At this point the review had found no clear evidence of corruption, but Statkraft had determined to report the case to Brazilian authorities. In addition, Statkraft announced that ØKOKRIM and the Norwegian Minister of Trade and Industry Monica Mæland have been informed, as the representative of the State.

C. Stakeholder Enforcement: 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 Government Pension Fund Global (“GPFG” or the “Fund”), which recommends whether the Fund 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 has become one of its priorities, and the recent uptick in the number of such corruption may have also been driven by the transfer of final decision-making power from the Ministry of Finance to the Norwegian Central Bank’s investment branch, Norges Bank Investment Management (“NBIM or the “Bank”).

1. The Fund and the Ethical Guidelines

The Norwegian Government Pension Fund Global (“GPFG” or “Fund”) 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 has the overall responsibility for the management of the Fund and has issued guidelines for its management. The Fund is managed by the Norwegian Central Bank (“Norges Bank” or “Bank”), whose Executive Board has delegated the operational management to Norges Bank Investment Management (“NBIM”).

In June 2017, the GPFG was the world’s third largest sovereign wealth fund, managing assets of more than USD 950 billion, with investments in just under 9,000 companies in 77 countries. It owns approximately 1.3% of the equity of listed companies on a worldwide basis, and 2.3% of the equity of listed European companies.

The Fund invests in equities, bonds and real estate globally, and consists of 60% equities, 35-40% fixed-income securities and up to 5% 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 the 2014 Guidelines for observation and exclusion of companies from the GPFG’s portfolio (“Ethical Guidelines”), as amended in 2017, 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 a negative conduct that meets certain criteria (“conduct-based exclusion”) for responsible investment.

With respect to product-based criteria, the Ethical Guidelines provide that the Fund shall not invest in companies who 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) mining or power-producing companies that directly or indirectly (through companies that they control) 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.

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 now led by Johan H. Andresen, a Norwegian industrialist and philanthropist. The Council's new 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 responsibility to continuously monitor the Fund's portfolio to identify companies that contribute to or are responsible for conduct which may justify observation or exclusion. The Council encourages individuals and organizations to provide information about cases that may be of relevance for 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 that 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 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 & 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, and 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 in the past been perceived 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 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 information and coordination to clarify their respective roles and responsibilities.

4. 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 below) have been fulfilled or any other uncertainty about the situation. The Council has stated that placement 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 would monitor (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.

To date, three companies have been placed under observation because of the risk of severe corruption. In 2009, Siemens AG was placed under a four-year observation term, which has since been lifted. In 2011, Alstom SA was placed under observation, and the observation was lifted in 2015. In 2015, Petrobras was also put under observation. In 2017, Leonardo SpA and PetroChina Ltd. were placed under observation for severe corruption.

5. Considerations for Exclusion

The Ethical Guidelines provides 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.” Before making a decision on observation and exclusion, the Bank must also evaluate “whether other measures, including the exercise of ownership rights, may be more suited to reduce the risk of continued norm violations, or whether such alternative measures may be more appropriate for other reasons.”

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. 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.

Companies are not excluded for a defined time period, 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.

6. Assessment of Future Risk in Corruption Cases

While not formally binding upon the Council, gross corruption is broadly defined to cover aggravated corruption within the meaning §§ 387 and 388 of the Norwegian Criminal Code, and 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.

Key to the second part of the test for exclusion as a result of gross corruption is whether the company has implemented an effective anti-corruption compliance program, and, 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 and 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 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, and 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 effectively assess risk 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.

In its 2016 annual report, the Council observed that the companies for which it had recommended observation between 2014 and 2016, generally did not recognize that they had a history of corruption, which was viewed as an attitude that may constitute an impediment to changing company culture. In addition, the Council was not convinced that formal changes in the companies' internal controls had been appropriate and effectively implemented. For cases that had resulted in exclusion, the Council had found that the companies had been involved in gross corruption and that there was a future risk of new violations, either because the companies failed to respond to the Council's inquiries, or that the companies had not substantiated that they had taken appropriate remedial steps, such as issuing disciplinary measures not only against individuals directly involved in corrupt practices, but also against senior managers who knew or should have known about these practices.

7. Decisions about 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 on 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 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 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 will 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."

8. Specific Corruption Cases 2016 – 2017

In 2016 and 2017, the Council on Ethics issued recommendations with respect to the observation or exclusion of four companies. As described below, two companies were placed under observation (PetroChina and Leonardo SpA), 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 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 substantiated 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, that company's lack of willingness to provide relevant information, in and of itself contribute 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 terms 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 presumes 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 side-step 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, as 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 for failing to provide appropriate anti-corruption training to such agents. Finally, and 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 follow-up on these issues through active ownership dialogue with Leonardo.

- *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, 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 have been or currently are 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 in 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 has 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 does not have appropriate corruption risk assessment processes, nor does 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 follow-up 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, an Italian multinational oil services

company, be placed under observation due to future risk of gross corruption. The Council noted that Saipem is 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 both through written communications and meetings, and Saipem provided comments to the draft recommendation, the Council 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 present-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 to several important subsidiaries, with the help of an external consultant. The Council therefore recommended to re-evaluate the situation in a couple of years. Norges Bank did not follow the Council's recommendation, and announced on May 5, 2017 that it decided to ask NBIM to follow up on the risk of corruption in its ownership dialogue with the company.

D. Stakeholder Enforcement: 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. As of June 2017, companies excluded on the basis of gross corruption were Centrais Eletricas Brasileiras SA (2016), China Railway Group Ltd (2015), Leonardo SpA (2017), PetroChina (2017), Petrobras (2016), and ZTE Corporation (2016). Several of these were excluded, expressly citing the Council's May recommendations to exclude. Interestingly, while the Fund did not necessarily end up excluding the companies, these companies were excluded by KLP. In total, KLP has excluded 174 companies for violations of KLP's Guidelines for Responsible Investments.

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. In total, almost 180 companies (including relevant named affiliates) and individuals have been added to the MDB cross-debarment list so far in 2017 for misconduct on international development projects.

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 the largest of the World Bank’s 14 global practices (which have replaced the Bank’s previous six regional departments).

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.

Interestingly, 2016 saw the birth of a new MDB: the Asian Infrastructure Investment Bank (“AIIB”), declared open for business on January 16, 2016. First proposed in 2013 by the government of the People’s Republic of China, the AIIB’s declared goal is to support infrastructure development and regional connectivity in the Asia-Pacific region. With its initial capital of \$100 billion and a membership roster including over a quarter of the world’s nations and 16 of the world’s 20 largest economies, including Britain, Germany, Australia, and South Korea, the AIIB is poised to play a major role in the Asian infrastructure financing sector (a first joined-loan with the ADB was announced in March 2016). On the anti-corruption front, the AIIB is developing a special compliance-and-integrity unit that will oversee its management and report directly to the AIIB’s board. The AIIB also has a sanctions regime, which appears designed to share many common features with the regimes of other major MDBs. In March 2017, the AIIB 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 statistics, in fiscal year 2016 alone, the World Bank investigated 124 contracts and 43 projects, worth \$633 million, pursuant to allegations of sanctionable practices. Between 2012 and 2016, the World Bank sanctioned 329 firms and individuals through its Sanctions Procedures. By way of comparison, the ADB had, as of May 31, 2016, imposed sanctions on 444 firms and 497 individuals in addition to honoring cross-debarments for firms and individuals.

The increase in sanctioning activity, the potential disruptions caused by the sanctions procedures, as well as the severity of sanctions, underscores the growing 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 April 15, 2012 version of the Sanctions Procedures.

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, 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 choose to bypass the OSD and file a written “Response” directly with the Sanctions Board, within 90 days of the receipt of the Notice. As of 2015, two-thirds of all cases (67%) were resolved at the level of the OSD and only one-third (33%) proceeded to the Sanctions Board.

Sanctions Board: The Sanctions Board is the final adjudicator of contested cases. The Board is also the first non-purely Bank affiliated body to review the case: unlike the OSD, which is composed entirely of World Bank-appointed staff, four of the Sanctions Board’s seven members are external (*i.e.*, have never held a World Bank position); the remaining three are 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 (which includes the “Response” submitted by respondents and a “Reply” submitted by INT). 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 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)).

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 which can be 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 shared only with the limited number of persons specified in the Sanctions Procedures.

Since 2009, the OSD also has (and increasingly uses) 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 2009, INT began to resolve some of its investigations through negotiated resolution agreements (“NRAs”). In 2016, 18 of the 58 sanctions imposed were imposed pursuant to such NRAs³⁴. INT and the company/individual alleged to have engaged in the misconduct 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, more recently, the April 2015 settlement with French global telecommunications equipment company Alcatel Lucent. Alcatel had been under investigation for the failure of two of its Egyptian and Italian subsidiaries to disclose agents, which had been hired on behalf of two other Alcatel subsidiaries (Alcatel-Lucent Trade International A.G. and Alcatel Saudi Arabia Limited) to assist in securing \$30 million worth of telecommunications services and training contracts in 2006. While the terms of the NRA foresaw a conditional non-debarment for four implicated Alcatel subsidiaries (including the Italian and Egyptian subsidiaries), Alcatel-Lucent Trade International A.G. and Alcatel Saudi Arabia Limited were debarred for a period of 18 months by the World Bank (and, by virtue of the Cross-Debarment Agreement, by other MDBs).

B. AfDB Sanctions Regime

The AfDB’s sanctions system is currently laid out in the November 2014 version of the 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”))

³⁴ INT Report 2016, page 27. <http://pubdocs.worldbank.org/en/118471475857477799/INT-FY16-Annual-Update-web.pdf>

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.

Variations worth pointing out include the difference in standard for the granting of early temporary suspensions. 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). This requirement of imminent harm brings the AfDB's procedures in line with generally accepted standards for issuing retraining-type orders, unlike the World Bank sanctions procedures (discussed *supra*). Another difference relates to the availability of hearings. Under the World Bank sanctions regime, respondents may request a hearing which will be granted 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 IACD 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 August 2017, the AfDB debarred Chinese state-owned Chongqing International Construction Corporation ("CICO") for twelve months in connection with fraudulent practices committed by CICO on an AfDB road project in Uganda. According to the AfDB's announcement, CICO inflated its experience, overstating both the scope and value of past contracts in order to meet the qualifications for the road project in Uganda. The AfDB indicated that CICO'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." The most recent version of these procedures took effect in November 2015 and brought with it a number of significant changes. Perhaps most importantly, while the old Procedures only foresaw one level of adjudicative review by the so-called "Enforcement Committee," the new Procedures create a two-tiered adjudicatory process by adding the initial review of the "Enforcement Commissioner." The new Procedures also increase the independence of the Enforcement Committee: while its five members were previously internal to the Bank, the new Procedures dictate that three out of the five members must be external to the Bank. Moreover, decisions of the Enforcement Committee are now final and no longer subject (as before) to the referral to the Bank's President or Executive Committee. Another important change relates to the new ability of the EBRD's investigative body (the "Office of the Chief Compliance Officer") to enter into negotiated resolution agreements with the parties: previously, even when the parties agreed, settlements were not foreseen by the previous version of the Procedures. Finally, in a greater push for transparency, the EBRD has decided that going forward, it would publish on the Bank's website any enforcement actions leading to debarments or debarments with conditional release (decisions where the EBRD issues other types of sanctions will not be published but may be disclosed as the Bank deems appropriate).

Inter-American Development Bank: The IDB's sanctions process underwent a major revision in 2011, which brought it mostly in line with the sanction processes of other MDBs. Specifically, the 2011 revision created a two-tier adjudicative system composed of the so-called "Case Officer" and the "Sanctions Committee," charged with resolving cases brought by the Bank's investigative body, called the "Office of Institutional Integrity." The IDB's sanctions regime was revised once more and the newest version of the sanctions procedures came into effect on June 9, 2015. Aside from select terminological changes (e.g., the "Case Officer" is now called the "Sanctions Officer"), the latest amendments have introduced the concept of negotiated settlements into the IDB's sanction process (see new article 15.4) and now provide respondents with the opportunity to contest the case prior to the decision by the Sanctions Officer (the previous version of the procedures allowed only appeals to the Sanctions Committee). Moreover, under the new sanctions process, the IDB must publish on its website all sanctions imposed by the Sanctions Officer and the Sanctions Committee but continues to maintain discretion as to whether or not to disclose the identity of the sanctioned party or the details about the underlying misconduct.

Asian Development Bank: Updates to the Asian Development Bank's Integrity Principles and Guidelines ("Guidelines") were approved in 2014 and became effective on January 1, 2015. Like the World Bank's Sanctions Procedures, the 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"). Under the previous version of the Guidelines, the Head of the OAI also acted as the Secretariat to the Sanctions Appeals Committee. In order to ensure greater independence from the investigation process, the new Guidelines mandate that the Sanctions Appeals Committee's Head be picked from senior ADB staff, external to the OAI. Unlike the EBRD and the IADB,

the ADB has—in this latest round of revisions—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.

AIB: The AIB's sanctions process is set out in the Bank's Policy on Prohibited Practices, which was released on December 8, 2016. The AIB's process is largely modeled on the World Bank's system, providing for a two-tiered adjudicatory system. At the first stage, the AIB'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.

IV. Mitigation of Potential Sanctions: 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, including with respect to the initiatives and remedial actions that it expects from companies and individuals to receive mitigating credit.

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 months 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.

A. 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 employees 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).)

B. 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*.

C. 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, 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).)

D. 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 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).)

V. A Growing Trend of 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. The World Bank, for instance, has signed over 40 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 2016 alone, the World Bank made a total of 62 referrals. Notably, referrals made in 2016 and previous years have led to the prosecution and conviction of at least 35 individuals and to criminal charges brought against an additional 29 individuals.

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

1. Dutchmed BV

The recent 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.

2. SNC-Lavalin

The matter of Canadian engineering firm SNC-Lavalin, which INT's Vice President Leonard McCarthy called "a testimony to collective action against global corruption," has become the most emblematic case illustrating the potentially wide-reaching effects caused by MDB referrals to national authorities. What began in 2010, with an investigation by INT into a World Bank-financed project in Bangladesh was referred to national authorities and grew to encompass several investigations and proceedings in multiple jurisdictions, some of which are still ongoing. The matter even reached the Canadian Supreme Court in the context of a high-profile case regarding the Bank's institutional immunity and privileges, which had the potential to significantly impact the Bank's referral program.

a. Overview of the matter

In 2010, based on information from "tipsters" (as they came to be called in the proceedings that followed), the Bank began an investigation into allegations of corruption surrounding SNC-Lavalin's bid for the multimillion-dollar Padma Bridge construction project in Bangladesh. In 2011, a few months into

the investigation, INT found that there was sufficient credible evidence to refer the matter to the Royal Canadian Mounted Police (“RCMP”). Based on this referral, the RCMP started its own investigation into potential violations by SNC-Lavalin under the Canadian Corruption of Foreign Public Officials Act. The RCMP investigation was marked by several raids of SNC-Lavalin offices, further collaboration between the RCMP and the World Bank, and cooperation with enforcement authorities in other jurisdictions, including Switzerland. Beyond SNC-Lavalin’s conduct in Bangladesh, Canadian and Swiss authorities investigated allegations of money laundering and bribery relating to SNC-Lavalin contracts in multiple countries, including Canada, Algeria and Libya, where—as was later revealed—an SNC-Lavalin executive was alleged to have arranged more than \$160 million in bribes to the son of former Libyan leader Moammar Gadhafi.

In March 2012, while a number of these external investigations were ongoing, SNC-Lavalin’s CEO, Pierre Duhaime, resigned from his position, after an internal company probe concluded that he had approved US\$56 million of questionable payments in violation of SNC-Lavalin’s code of ethics. Mr. Duhaime’s resignation was followed by the arrests of—and criminal charges being brought against—multiple former SNC-Lavalin executives, including Mr. Duhaime himself, in 2012 and 2013.

The multi-jurisdictional investigation efforts which followed the World Bank’s referral prompted the World Bank to suspend payment of the Padma Bridge Project in October 2011. In April 2013, the World Bank reached a settlement with SNC-Lavalin, imposing a ten-year debarment on the company and on over 100 of its affiliates for the company’s conduct in Bangladesh as well as conduct in Cambodia (of which the Bank had learned while the investigations were ongoing).

b. Threat to MDB’s Immunity and Privileges

Amidst the plethora of proceedings and investigations that have plagued SNC-Lavalin over the past years, the case brought by Canada against Kevin Wallace, Ramesh Shah and Mohammed Ismail (three former SNC-Lavalin executives), as well as Zulfiquar Bhuiyan, (a former agent of SNC-Lavalin in Bangladesh), received the most scrutiny from the compliance community. Indeed, these proceedings almost led to a precedent limiting the institutional immunity and privileges enjoyed by MDBs in the context of international cooperation, which, in turn, would have significantly impacted MDB referral practices.

The proceedings began in early 2012 when Canada brought criminal charges against Messrs. Ismail and Shah under Canada’s Corruption of Foreign Public Officials Act; Messrs. Wallace and Bhuiyan were charged in September 2013. During the ensuing trial, Canada intended to use evidence that the RCMP had obtained through wiretapping SNC-Lavalin’s offices. The authorization for the wiretaps had in turn been authorized in part on the basis of information which INT had shared with the RCMP.

Kevin Wallace and the others accused fought the charges brought against them by questioning whether the wiretaps used by the RCMP and authorized based on INT’s investigative findings were legally obtained. As part of this challenge, lawyers for the accused sought an order requiring production of INT’s investigative file and the validation of subpoenas issued to two INT investigators. The World Bank refused to turn over the file and to comply with the subpoenas, invoking the immunity of its archives and the immunity and privileges of its officers and employees (embedded in Articles VII and VIII of the World Bank’s Articles of Agreement).

The challenge was first brought before the Ontario Supreme Court Judge Ian Nordheimer, who, in December 2014, issued a decision siding with the accused. While recognizing that the Bank enjoyed institutional immunity from the jurisdiction of the Ontario Superior Court *prima facie*, Judge Nordheimer determined that the immunity had been “impliedly” waived by the Bank as a result of its extensive cooperation with Canadian authorities. Judge Nordheimer thus ordered the Bank to produce its records.

The Bank appealed the Ontario Superior Court’s decision to the Supreme Court of Canada, who granted the Bank’s application for leave (equivalent of a *writ of certiorari*) in July 2015. Prior to the hearing, a number of other MDBs and international institutions, including Transparency International, submitted *amicus curiae* briefs warning of the “chilling effect” a failure to uphold institutional immunity would have on MDB cooperation with national enforcement authorities. In fact, pending the resolution of this matter, the Bank and other MDBs reportedly either halted or drastically reduced referrals to national authorities.

On April 29, 2016, Canada’s Supreme Court issued its decision in *World Bank Group v. Wallace* and, much to the relief of the Bank and other MDBs, ruled in favor of the Bank. Specifically, the Supreme Court held that there had been no implied waiver of the immunities and privileges applicable to the Bank’s archives and personnel and that, consequently, INT could not be obligated to make its staff and investigative file available. Underscoring the importance of the concept of immunity, and in particular the inviolability of archives as “integral to the independent functioning of international organizations,” the Supreme Court recognized that limiting such immunity would thwart the global fight against corruption because “[MDBs] including the World Bank Group are particularly well placed to investigate corruption and to serve at the frontlines of international anti-corruption efforts.”

c. Coordinated Relief

Against this backdrop, it should nevertheless be noted that collaboration between the MDBs and national authorities can, in certain cases, have a simplifying effect for companies already involved in debarment or sanctions proceedings. In the case of Alstom SA, the U.S. Department of Justice declined to impose a corporate monitorship in its 2014 plea agreement with the company, so long as the company satisfied the World Bank Integrity Compliance Office monitoring requirements. Under the terms of its Deferred Prosecution Agreement, which credited the compliance enhancements the company had already made under its World Bank resolution, Alstom was allowed to self-report as to the status of the implementation of its compliance program and internal controls so long as the ICO’s requirements, which included a “Corporate Compliance Program that complies with the World Bank’s integrity compliance policies and practices, particularly those reflected in the World Bank’s Integrity Compliance Guidelines,” were satisfied. As of February 21, 2015, the ICO concluded that Alstom had satisfied all the requirements and conditions of its 2012 settlement with the World Bank.

CHAPTER 6: OTHER INTERNATIONAL DEVELOPMENTS

I. ISO 37001

A. *Introduction*

In October 2016, the International Organization for Standardization (“ISO”) issued the ISO 37001 Anti-Bribery Management Systems Standard (“Standard”) setting forth an international anti-bribery management system standard reflecting international best practices for managing bribery risks as well as setting forth the minimum anti-bribery compliance requirements. The Standard provides guidance for establishing, implementing, maintaining, reviewing and improving an anti-bribery management system and was designed to be applied across jurisdictions, by organizations of any kind and size. Most notably, the Standard offers participants a certificate issued by an independent third party as a validation of its anti-bribery compliance program.

The Standard only applies to bribery, and does not address fraud, cartels, money laundering, and other corrupt practices. This summary first discusses the key features of the Standard, followed by a discussion of the certification process.

B. *ISO 37001 Key Features*

A number of features are worthy of mentioning:

- **Section 4.5 Anti-Corruption Risk Assessment:** Section 4 addresses the need to understand the organization to establish an effective, tailored anti-bribery program. Section 4.5 provides that organizations must undertake regular bribery risk assessments to analyze, assess, and prioritize potential bribery risks, which should be mitigated by appropriate controls.
- **Section 5.1.2 Anti-Bribery Policies and Objectives:** Section 5 addresses the importance of commitment by senior management to maintaining an anti-bribery culture, which includes establishing, implementing, maintaining, and reviewing policies and objectives that adequately address the organization’s bribery risks. Such policies should be communicated in the appropriate language and to business associates who pose heightened risk of bribery.
- **Section 7.3 Awareness and Training:** Section 7 addresses the importance of having sufficient, competent support and resources for the anti-bribery management system. Section 7.3 specifies the need for regular and appropriate training to personnel about the organization’s anti-bribery policies and procedures and ways to recognize solicitations and bribes. Such support also includes proper documentation of the organization’s anti-bribery management system, which means ensuring that the documented information is available and suitable for use, where and when it is needed. Additionally, conditions of employment should be contingent on personnel complying with anti-bribery policies.
- **Section 8.1 Operational Planning and Control:** Section 8 addresses the need for the organization to implement controls to mitigate bribery risks, including conducting proper due diligence on transactions and activities and relationships; implementing financial and non-financial controls; establishing procedures designed to prevent offering, providing, and accepting gifts, hospitality, or

donations that could be perceived as bribery; maintaining channels for persons to raise concerns, including anonymous reporting; and implementing investigation procedures and ways to deal with bribery.

- Section 9.2 Internal Audit: Section 9 deals with the importance of evaluating and monitoring the organization's anti-bribery management system, which includes using an internal audit to conduct reasonable, proportionate, risk-based audits to review procedures and controls relating to bribery to identify any weaknesses and opportunities for improvement.
- Section 10.2 Continual Improvement: Sections 10 and 10.2 specify the need for the organization to continually improve the suitability, adequacy and effectiveness of its anti-bribery management system.

C. Certification by Accredited Third Parties

Companies can obtain an ISO 37001 certification from accredited third parties to attest to the quality of its anti-bribery management system. Since its issuance, several companies, including Wal-Mart, Microsoft, Alstom, and ENI (Italy), have announced that they have a certificate or are in the process of seeking certification. Along with these multinational companies, Singapore, Peru, and Ecuador have adopted the standard giving rise to the expectation that this will lead to other countries joining the trend.

Certification is provided by qualified auditors, who carry out in-depth site visits including visits to headquarters and regional and subsidiary offices to interview top management and other departments (such as sales, HR, Legal, and Audit) and test on a sample basis anti-bribery controls to assess the quality of the anti-bribery management system. The review scope will vary depending on the auditors, but generally will include site visits, interviews, data mining, sample testing of compliance sensitive transactions, assessment of internal controls, and analysis of interactions with high-risk third parties.

II. E.U. Data Protection Developments

Data protection has grown in importance in the past decade, and is a subject of great importance to Europeans in particular. This section discusses two separate currents of legal developments related to data privacy. Section 1 discusses the E.U. General Data Protection Regulation ("GDPR"), enacted in April 2016, which strengthened the protections of personal data within the E.U. Section 2 discusses issues that have arisen with the need to transfer personal data between the E.U., where data protections are generally stronger, and the United States, which led initially to the creation of the Safe Harbor regime. After the Safe Harbor regime was invalidated by the European Court of Justice, it was replaced in 2016 by a new Privacy Shield regime, although it remains an open question whether the Privacy Shield (as enacted) will survive legal scrutiny in the E.U.

A. The E.U. General Data Protection Regulation

In April 2016, after four years of preparation to overhaul the European Union's data protection rules, the members of the E.U. Parliament gave final approval to the E.U. General Data Protection Regulation ("GDPR"). The GDPR's stated aims are to return control of personal data to citizens and to simplify regulations. This new set of rules is a modernization of the data protection regime established by Directive 95/46/EC, which dates to 1995. The GDPR came into force in May 2016, and member states

have two years to comply. To better understand the 2016 modernization, we will briefly explore the contours of the 1995 Directive it 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 restricts 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 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 encompasses essentially every action taken in connection with U.S. discovery, including “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.” Personal data should not be processed at all, except when three conditions are met: (i) transparency, (ii) legitimate purpose, and (iii) proportionality. Accordingly, (i) the data subject has the right to be informed when his or her personal data is being processed; (ii) personal data can only be processed for specific explicit and legitimate purposes; and (iii) personal data may 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 is strictly prohibited when the data is intended to be transferred to non-E.U. countries, except if the recipient country provides 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 requires each EEA country to enact data protection laws that are 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 EEA, 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 E.U. General Data Protection Regulation, or GDPR.

B. 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 is intended to enable people to better control their personal data. On the other hand, the **Data Protection Directive** will require the E.U. members 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 shall apply from May 25, 2018. The Directive entered into force on May 5, 2016 and E.U. Member States have to transpose it into their national law by May 6, 2018.

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, it being noted that the existing Directive 95/46/EC will be repealed once the GDPR comes into effect;
- Introduces higher sanctions (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;
- Broadens the territorial scope of data protection laws 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. (standing 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. For the first time, data processors must (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;
- 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;
- Clarifies the consent required from data subjects. Such consent could previously be assumed in certain circumstances, but now consent must 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;
- Increases transparency obligations within privacy notices, such that existing forms of fair processing notice will have to be re-examined;
- 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 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.

C. 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., where data privacy protections are generally more robust, 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 framed the transfers of private 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 of personal data transferred from the E.U., and as a result, personal data could be freely 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:

- Data transfers can no longer be based on the Commission's invalidated Safe Harbor Decision;
- Standard Contractual Clauses [] and Binding Corporate Rules [] can in the meantime be used as a basis for data transfers....

3. The 2016 Privacy Shield: A Safer Safe Harbor?

In a July 12, 2016 decision, the European Commission essentially approved the 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 [“Privacy Shield”] from the [European] Union to self-certified organizations in the United States.” 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 by 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.

As evidence that the Snowden revelations still reverberate in Europe, 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 July 26, 2016, the Article 29 Working Party issued a statement that commended the work done to achieve the Privacy Shield including through considering various concerns raised by the Working Party in the past, but fell short of a full-throated endorsement of the Privacy Shield, stating that “a number of [Working Party] concerns remain.”

The Working party stated that it “would have expected stricter guarantees concerning the independence and the powers of the Ombudsperson mechanism. Regarding bulk collection of personal data, the WP29 notes the commitment of the ODNI not to conduct mass and indiscriminate collection of personal data. Nevertheless, it regrets the lack of concrete assurances that such practice does not take place.” Rather than fully endorse (or reject) the Privacy Shield, the Working Party stated that it would withhold further judgment until the first joint annual review to “assess if the remaining issues have been solved [and] if the safeguards provided under the E.U.-U.S. Privacy Shield are workable and effective.”

Since the Working Party’s July 2016 statement, the first joint annual review of the Privacy Shield was conducted. In a joint statement issued on September 22, 2017, the E.U. Commissioner for Justice, Vera Jourová, and U.S. Secretary of Commerce Wilbur Ross announced that, “The Privacy Shield raised the bar for transatlantic data protection by ensuring that participating companies and relevant public authorities provide a high level of data protection for E.U. individuals.” The statement went on to affirm that both the United States and the European Union “remain committed to continued collaboration to ensure [the Privacy Shield] functions as intended.” It remains to be seen how the results of this first joint annual review will be received by the Working Party.

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 European Court of Justice 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. In addition, critics fear that the new U.S. Ombudsman will lack the true independence and authority to serve as a check and balance against overbroad collection of E.U. personal data by the U.S. intelligence community. Max Schrems, the eponymous *Schrems* plaintiff who continues to be active as a privacy advocate, has argued that “the Privacy Shield must comply with the criteria defined by the E.U. and its courts of justice, which clearly indicated that the mass collection of personal information is not compatible with the fundamental personal data protection rights.” Time will tell whether *Schrems*, which invalidated the Safe Harbor, will be followed by a *Schrems II* challenging the Privacy Shield.

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 European Union 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.

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.